BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE DIRECTORY 33-303

1 NOVEMBER 1999

Communications and Information

COMPENDIUM OF COMMUNICATIONS AND INFORMATION TERMINOLOGY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AFCA/XPXP (Mr. Johan Dekker)	Certified by: HQ USAF/SCXX (Lt. Col. Terry G. Pricer Sr.)
Supersedes AFDIR 33-121, 1 November 1997; and AFMAN 33-270, 8 August 1994.	Pages: 209 Distribution: F

This Air Force directory (AFDIR) identifies abbreviations, acronyms, and terminology most commonly used by the Air Force communications and information, and information assurance (IA) communities. It is not all encompassing, but will assist the user in researching unfamiliar terms. Use this directory as a source document when a standard communications or information-related acronym or definition is needed. Send recommended changes or comments to HQ AFCA/XPXP, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using Air Force Form 847, **Recommendation for Change of Publication**.

SUMMARY OF REVISIONS

This publication implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; AFPD 33-2, *Information Protection*; and AFPD 37-1, *Air Force Information Management* (will convert to AFPD 33-3, *Information Management*). This publication combines the revised contents of AFDIR 33-121, *Compendium of Communications and Information Terminology*; and Air Force Manual (AFMAN) 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*, and adds selected computing and networking acronyms and terminology.

1. Introduction . There are a number of different glossaries and other documents published within the Federal government, DoD, and the Air Force that list terms and definitions. This directory is designed to help minimize the differences and conflicts between communications and information and IA terms, to standardize them as much as possible, and reduce unnecessary proliferation.

2. Scope . The focus of this compendium is on communications and information, and IA terms, not on general purpose Air Force or major command (MAJCOM) unique terms. MAJCOMs may supplement abbreviations, acronyms, and terms specific to their commands. **Attachment 1** contains communications and information abbreviations, acronyms, and terminology; **Attachment 2** contains IA abbreviations, acronyms, and terminology. As a general guideline, with few exceptions, the following items are not included: Air Force organizations and descriptions of their missions and functions; names and descriptions of Air Force, Joint, or DoD management programs or projects; miscellaneous communications systems/equipment descriptions and nomenclatures, and computer software programs. For everyday Air Force use, the term communications and information system replaces similar previous terms such as: communications-computer system (C-CS), command, control, communications, and computers (C4), information system (IS), and automated information system (AIS), except in those cases where the definition containing one of these terms is an approved Joint, DoD, or National-level definition.

WILLIAM J. DONAHUE, Lt. Gen., USAF
Director, Communications and Information

Attachment 1

COMMUNICATIONS AND INFORMATION TERMINOLOGY

Abbreviations and Acronyms

AAL—Asynchronous Transfer Mode (ATM) Adaptation Layer

ACE—Adaptive Communications Element

ACMIS—Automated Configuration Management/Integration System

ACMS—Advanced Configuration Management System

ACOC—Area Communications Operations Center

ACOT—Advanced Communications Officer Training

ACP—1. Allied Communications Publication
2. Associated Control Protocol
3. Automatic Communications Processor

ACSU—Advanced Channel Service Unit

ACTS—Automated Circuit Testing System

ACU—Automatic Calling Unit

A/D—Analog-to-Digital

ADCCP—Advanced Data Communication Control Procedures

ADCON—Administrative Control

ADENS—Advanced Data Exchange Network System

ADFS—Automated Digital Facsimile System

ADL—Automatic Data Link

ADM—1. Add-Drop Multiplexers
2. Advanced Development Model

ADMS—Automatic Digital Message Switch

ADN—Advanced Digital Network

ADNX—Analog/Digital Network Exchange

ADP—Automated Data Processing

ADPCM—Adaptive Differential Pulse Code Modulation

ADPE—Automated Data Processing Equipment

ADPF—Automated Data Processing Facility

ADPRMIS—Automated Data Processing Resource Management Information System

ADPS—Automated Data Processing System

ADPSEC—Automated Data Processing Security

ADPSO—Automated Data Processing Selection Office

ADRSS—Automated Data Reports Submission System

ADS—Automated Data System

ADSL—Asynchronous Digital Subscriber Line

ADU—Accumulation and Distribution Unit

ADWS—Automated Digital Weather Switch

AEHF—Advanced Extremely High Frequency

AES—Advanced Encryption Standard

AFADPP—Air Force Automated Data Processing Plan

AFC—Area Frequency Coordinator

AFCDAd—Air Force Component Data Administrator

AFCDD—Air Force Corporate Data Dictionary

AFCERT—Air Force Computer Emergency Response Team

AFCISP—Air Force Communications and Information Plan

AFCVIL—Air Force Central Visual Information Library

AFD—Automated File Designator

AFDD—Air Force Doctrine Document

AFDE—Air Force Data Encyclopedia

AFDIR—Air Force Directory

AFDSEC—Air Force Data Systems Evaluation Center

AFDSRS—Air Force Defense Software Repository System

AFEKMS—Air Force Electronic Key Management System

AFETS—Air Force Engineering and Technical Service

AFFORMS—Air Force Forms

AFHAN—Air Force Handbook

AFHIS—Air Force Headquarters Information System

AFHOI—Air Force Headquarters Operating Instruction

AFI—Air Force Instruction

AFIMS—Air Force Information Management System

AFINTNET—Air Force Intelligence Network

AFIRDS—Air Force Information Resources Dictionary System

AFIWC—Air Force Information Warfare Center

AFJI—Air Force Joint Instruction

AFLANSPO—Air Force Local Area Network System Program Office

AFMAN—Air Force Manual

AFMIS—Air Force Major Command Information System

AFNET—Air Force Network

AFNMS—Air Force Network Management System

AFNCC—Air Force Network Control Center

AFNOC—Air Force Network Operations Center

AFODMSS—Air Force Office Data Management Security System

AFOLDS—Air Force On-Line Data System

AFPAM—Air Force Pamphlet

AFPD—Air Force Policy Directive

AFPDC—Air Force Publishing Distribution Center

AFRSN—Air Force RED Switch Network

AFRTS—Armed Forces Radio and Television Service

AFSATCOM—Air Force Satellite Communications System

AFSCF—Air Force Satellite Control Facility

AFSCN—Air Force Satellite Control Network

AFSN—Air Force Systems Networking

AFSPOC—Air Force Space Operations Center

AFT—Asynchronous File Transfer

AF/VAS—Air Force Value Added Software

AGC—Automatic Gain Control

AHF—Adaptive High Frequency

AIDES—Analyst Intelligence Display and Exploitation System

AIG—Address Indicator Group

AIM—AFSATCOM/IEMATS Microprocessor

AIMS—Automated Information Management System

AIRPS—Air Postal Squadron

AISARC—Automated Information Systems Acquisition Review Council

AITI—Automated Interchange of Technical Information

AJ—Anti-Jam

ALE—Automatic Link Establishment

ALG—Application Layer Gateway

ALGOL—Algorithmic Language

ALN—Access Location Number

ALOC—Air Lines of Communication

ALS—Ada Language System

ALTA—Advanced Lightweight Tactical Antenna

AM—Amplitude Modulation

AMA—Automatic Message Accounting

AMD—Advanced Micro Devices

AME—Antenna-Mounted Electronics

AMHS—Automated Message Handling System

AMI—Alternate Mark Inversion

AMIS—Automated Management Information System

AMMUS—Air Force Minicomputer Multi-User System

AMMUSNET—Air Force Minicomputer Multi-User System Network

AMPE—Automated Message Processing Exchange

AMPS—Advanced Mobile Phone Service

AMS—Audiovisual Multimedia Services

AMSDS—Automated Management Supporting Data System

AMT—Aerial Mail Terminal

A/N—Alphanumeric

ANDVT—Advanced Narrowband Digital Voice Terminal

ANI—Automatic Number Identification

ANSI—American National Standards Institute

AO—1. Authorized Outage
2. Area of Operations

AOSS—Automated Office Support System

AP—1. Application Profile
2. Application Protocol

APACCS—Aerial Port Automated Command and Control System

APF—Automated Processing Format

API—Application Programming Interface

APPC—Advanced Program-to-Program Communication

APS—Automatic Protection Switching

ARPC—Air Reserve Personnel Center

ARSTU—Auto Remote Secure Terminal Unit

ARU—Antenna Reference Unit

ASCII—American Standard Code for Information Interchange

ASCT—Auxiliary Satellite Control Terminal

ASDCS—Automated Source Data Collection System

ASG—Architecture Steering Group

ASIT—Adaptive Surface Interface Terminal

ASM—Administrative Support Manual

ASNC—Alternate SATCOM Network Controller

ASSA—Automated Support Systems Architecture

ATAM—Automated Threat Assessment Methodology

ATD—Advanced Technology Demonstration

ATDM—Asynchronous Time-Division Multiplexing

ATE—1. Asynchronous Terminal
2. Automated Test Equipment

ATIS—Automated Terminal Information System

ATM—Asynchronous Transfer Mode

ATW—Analog Trunked Wideband

AV—Audiovisual

AVD—Alternate Voice Data

AVR—1. Alternate Voice Record
2. Advanced VLF/LF Receiver

AWDS—Automated Weather Distribution System

AWN—Automated Weather Network

BAM—Basic Access Module

BASIC—Beginners All-Purpose Symbolic Instruction Code

BBP—Baseband Processor

BBS—Bulletin Board Service (System)

BCI—Bit Count Integrity

BCL—Binary Cutter Location

BCLD—Binary Cutter Location Data

BCRDR—Bar Code Reader

BCSA—Base-Level Communications-Computer Systems Assessment

BCUS—Basic Computer User Skills

BDN—Bulk Data Network

BDS—1. Base Distribution
2. Broadband Distribution System

BER—Bit Error Rate

BERT—Bit Error Rate Test

BERTS—Bit Error Rate Test Set

BIAO—Base Information Assurance Officer

BII—Base Information Infrastructure

BIOS—Basic Input/Output System

BIP—Base Information Protection

B-ISDN—Broadband-Integrated Services Digital Network

BISS—Base and Installation Security System

bit—Binary Digit

BIT—Built-In Test

BITC—Base Information Transfer Center

BITE—Built-in Test Equipment

BITS—Base Information Transfer System

BIU—Bus Interface Unit

BLISS—Base-Level Integrated Support System

BLOB—Binary Large Object

BLSR—Bi-directional Line Switched Ring

BMH—Base Message Host

BMTA—Backbone Message Transfer Agent

BOM—Bit-Oriented Message

BOSS—Basic Operating System Software

BPAC—Budget Program Activity Code

BPID—Blueprint Phased Implementation Directive

BPS—Bits Per Second

BPSK—Binary Phase Shift Keying

BRI—Basic Rate Interface

BSC—Binary Synchronous Communications

BSFT—Byte Stream File Transfer

BSHR—Bi-directional Self Healing Ring

BSS—Base Switching System

BTC—Base Telecommunications Center

BTS—Base Telephone System

BVIC—Base Visual Information Center

BVIM—Base Visual Information Manager

BVISC—Base Visual Information Support Center

C2—Command and Control

C2IPS—Command and Control Information Processing System

C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CAD—Computer-Aided Design

CADD/GIS—Computer-Aided Design and Drafting/Geographic Information System

CADDS—Computer-Aided Drafting/Design System

CAE—1. Computer-Aided Engineering
2. Common Applications Environment

CAEWIS—Computer-Aided Electronic Warfare Information System

CAFMS—Computer-Assisted Force Management System

CAI—Computer-Aided Instruction

CAIS—Computer-Assisted Instruction System

CAM—Computer-Aided Manufacturing

CAR—Customer Account Representative

CARDS—Comprehensive Approach to Reusable Defense Software

CASE—Computer-Aided/Assisted Software Engineering

CAT—1. Cable and Antenna Team
2. Computer-Aided Testing

CATV—Cable Television

CBCSS—Combat Communications Support Squadron

CBI—Computer-Based Instruction

CBT—1. Computer-Based Training
2. CSP Backside Terminal

CC—Common Carrier

CCA—Circuit Card Assembly

CCB—Configuration Control Board

CCC—Communications Common Carrier

CCD—Charge Coupled Device

CCE—Contingency Communications Element

CCEB—Combined Communications-Electronics Board

CCF—Consolidated Computer Facility

CCG—Combat Communications Group

CCI—Controlled Cryptographic Item

CCIR—International Radio Consultative Committee

CCIRC—CONUS Cable Installation Requirements Contract

CCIS—Command and Control Information System

CCITT—Committee Consultatif International de Telegraphique et Telephonique (International Telegraph and Telephone Consulting Committee)

CCO—Commercial Communications Office

CCS—Command and Control System

CCSD—Command Communications Service Designator

CCTV—Closed Circuit Television

CCWO—Commercial Communications Work Order

CD—Compact Disk

C-E—Communications-Electronics

CD-I—Compact Disk Interactive

CD-R—Compact Disk-Recordable

CD-ROM—Compact Disk-Read-Only Memory

CD-RW—Compact Disk-Re-writeable

CD-V—Compact Disk-Video

CD-WO—Compact Disk-Write Once

CD-WORM—Compact Disk-Write Once-Read Many

CD-XA—Compact Disk-Extended Architecture

CDA—Central Design Activity

CDAd—Component Data Administrator

CDBS—Common Data Base System

CDE—Common Desktop Environment

CDL—Common Data Link

CDMA—Code Division Multiple Access

CDPD—Cellular Digital Packet Data

CDOCS—Contingency DSCS Operations Control System

CDPS—Common Digital Data Preparation System

CDR—Combat Deployable Radio

CEMI—Communications-Electronics Maintenance Instruction

CEOI—Communications-Electronics Operating Instruction

CERT—Computer Emergency Response Team

CFE—Contractor Furnished Equipment

CFEP—Communications Front End Processor

CFM—Computer Facility Manager

CG—Communications Group

CGA—Color Graphics Adapter (or Array)

CGI—1. Computer Graphics Interface
2. Common Gateway Interface

CGM—Computer Graphics Metafile

CGP—Common Graphics Package

CHAT—Conversational Hypertext Access Technology

CI—1. Counterintelligence
2. Counterinformation

CIDE—Communications Interfaces and Data Exchange

CIM—Communications Improvement Memorandum

CIO—Chief Information Officer

CIP—1. Critical Infrastructure Protection
2. Crypto-Ignition Plug

CIRK—Common Interswitch Rekeying Key

CIRT—Computer Incident Response Team

CLIPS—Communications Link Interface Planning System

CLNP—Connectionless Network Protocol

CLNS—Connectionless Network Service

CLT—Communications Line Terminal

CLTP—Connectionless Transport Protocol

CLTS—Connectionless Transport Service

CM—Configuration Management

CMA—Control, Monitor, and Alarm

CMI—Computer-Managed Instruction

CMIP—Common Management Information Protocol

CMIS—Common Management Information Services

CMIS/P—Common Management Information Service and Protocol

CMO—Circuit Management Office

CMOS—Complimentary Metal-Oxide Semiconductor

CN—Communications Network

CNA—Computer Network Attack

CNCE—Communications Nodal Control Element

CND—Computer Network Defense

CNE—Computer Network Exploitation

CNIN—Composite Network Front End Internal Network

CNWDI—Critical Nuclear Weapon Design Information

CO—Central Office

COB—Collocated Operating Base

COBOL—Common Business Oriented Language

CODEC—Coder-Decoder

COE—Common Operating Environment

COM—Computer Output Microform

COMCAM—Combat Camera

COMINT—Communications Intelligence

COMJAM—Communications Jamming

COMM—Communications

COMOPS—Communications Operating Performance Summary

COMPES—Contingency Operation/Mobility Planning and Execution System

COMSAT—Communications Satellite

COMSATCOM—Commercial Satellite Communications

COMSEC—Communications Security

CP—Communications Processor

CP-SS—Central Processor Subsystem

CP/M—Computer Program/Microprocessor

CPC—1. Communications Payload Controller
2. Computer Program Component
3. Cross-Platform Communications

CPE—Customer Premise Equipment

CPIWI—Customer Premise Inside Wire Installation

CPM—Computer Performance Measurement

CPMF—Computer Program Maintenance Facility

CPPMO—Central Printing and Publications Management Organization

CPS—Characters Per Second Communications Processing System

CPU—Central Processing Unit

CRI—Collective Routing Indicator

CRLCMP—Computer Resources Life Cycle Management Plan

CRMA—Cyclic Reservation Multiple Access

CRT—Cathode Ray Tube

CRWG—Computer Resources Working Group

CRU—Computer Resource Utilization

CS—Communications Squadron

CSA—1. Cognizant Security Authority
2. Communications Service Authorization

CSB—Computer Support Base

CSC—1. Computer Software Component
2. Customer Service Center

CSCD—Cellular Switched-Circuit Data

CSCI—1. Commercial Satellite Communications Initiatives
2. Common Utilities Computer Software Configuration
3. Computer Software Configuration Item

CSCLS—Computational Support for Create Logistics Research

CSCPS—Cataloging and Standardization Center Provisioning System

CSIR—Communications and Information Systems Installation Record

CSM—Computer Systems Management

CSMA—Carrier Sense Multiple Access

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

CSO—Communications and Information Systems Officer

CSOM—Computer Systems Operator's Manual

CSP—Communications Support/System Processor

CSRD—Communications and Information Systems Requirement Document

CSS—Computer Systems Squadron

CSSO—Computer Systems Security Officer

CSU—1. Channel Service Unit
2. Communications Switching Unit
3. Computer Software Unit

CSU/DSU—Channel Service Unit/Data Service Unit

CT—Cellular Telephone

CTC—Combat Theater Communications

CTD—Common Tactical Dataset

CTI—Computer Telephony Integration

CTIS—1. Command Tactical Information System
2. Commander's Theater Information System

CTMC—Communications Terminal Module Controller

CTOS—Convergent Technologies Operating System

CTP—Common Tactical Picture

CTS—1. Clear-to-Send
2. Communications Technology Service
3. Conversation Time Sharing

CUA—Common User Access

CUI—Common User Interface

CW—Continuous Wave

DAA—Designated Approval Authority

DAC—Digital-to-Analog Converter

DACS—Digital Access Cross-Connect System

DAd—Data Administrator

DAL—Data Accessions List

DAMA—Demand Assigned Multiple Access

DAMPS—DDN Automated Message Processing System

DAP—1. Data Automation Proposal, Panel, or Plan
2. Document Application Profile

DAPM—Data Administration Program Manager

DAPMO—Data Administration Program Management Office

DASP—Data Administration Strategic Plan

DAT—Digital Audio Tape

DAVIS—Defense Automated Visual Information System

dB—Decibel

DB—Data base

dBm—Decibel (*referenced to 1 milliwatt*)

DBM—Data base Manager

DBMD—Data base Meta Dictionary

DBMS—Data base Management System

DBT—Data base Transfer

DBS—Direct Broadcast Satellite

DC—Direct Current

DCA—Distribution Communications Architecture

DCE—Data Circuit Terminating Equipment

DCC—Data Communications Channel

DCI—1. Defensive Counterinformation
2. Data Channel Interface

DCM—Data Communications Module

DCN—1. Design Change Notice
2. Digital Conventional Narrowband

DCO—Dial Central Office

DCP—Data Communications Processor

DCRSI—Digital Cassette Recording System, Incremental

DCS—1. Data Communications System
2. Digital Computer System

DCT—Data Communications Terminal

DCTN—Defense Commercial Telecommunications Network

DD—1. Data Dictionary

2. Department of Defense (*used on designated forms only*)

DDD—1. Data Description Document
2. Direct Distance Dialing

DDDS—Defense Data Dictionary System

DDF—Data Descriptive File

DDMA—Disk Directory Memory Access

DDN—Defense Data Network

DDP—Distributed Data Processing

DDRS—Defense Data Repository System

DDS—Data Dictionary System

DDT&E—Design, Development, Test, and Evaluation

DEA—Data Encryption Algorithm

DEB—Digital European Backbone

DED—Data Element Dictionary

DEMUX—Demultiplexer

DES—1. Data Element Standardization
2. Data Digital Encryption Standard

DFD—Data Flow Diagram

DHCP—Dynamic Host Configuration Protocol

DI—Data Integrity

DIB—Data Information Base

DIC—Document Identifier Code

DID—1. Data Item Description
2. Direct Inward Dialing

DIF—Digital Interface

DII—Defense Information Infrastructure

DIICC—Defense Information Infrastructure Control Concept

DISA—Defense Information Systems Agency

DISAN—Defense Information Systems Agency Notice

DISN—Defense Information Systems Network

DISNET—Defense Integrated Secure Network

DISS—Digital Ionospheric Sounding System

DIT—Directory Information Tree

DITPRO—DISA Information Technology Procurement Office

DITS—Digital Imagery Transmission System

DITSO—Defense Information Technology Services Organization

DIU—Data Interface Unit

DM—Domain Manager

DMATS—Defense Metropolitan Area Telephone Service/System

DMC—Defense Megacenter

DME—Distance Measuring Equipment

DMS—Defense Message System

DNS—1. Data Network System
2. Domain Name System

DNVT—Digital Nonsecure Voice Terminal

DOD—Direct Outward Dialing

DOS—Disk Operating System

DOV—Data Over Voice

DOW—Data Orderwire

DP&D—Data Processing and Display

DPA—Dual Phone Adapter

DPAS—Digital Patch and Access System

DPC—Data Processing Center

DPI—1. Data Processing Installation
2. Dots Per Inch

DPM—Dual Phone Modem

DPN—Digital Pipeline Network

DPSK—Differential Phase Shift Keying

DRAM—Dynamic Random Access Memory

DRFM—Digital Radio Frequency Memory

DRSN—Defense Red Switch Network

DS—Digital Signature

DSA—Directory Service Agent

DSAD—Data Systems Authorization Directory

DSC—DISN Service Center

DSCS—Defense Satellite Communications System

DSCSOC—Defense Satellite Communications System Operations Center

DSD—Data System Designator

DSDO—Data Systems Design Office

DSM—Digital Switching Module

DSN—Defense Switched Network

DSNET—Defense Secure Network

DSRS—Defense Software Repository System

DSS—1. Digital Switching System
2. DISN Switched Services

DSSO—Data System Support Office

DSTE—Digital Subscriber Terminal Equipment

DSU—1. Data Service Unit
2. Digital Service Unit

DSVT—Digital Subscriber Voice Terminal

DT&E—Development, Test, and Evaluation

DTC—Data Transfer Cartridge

DTD—Data Transfer Device

DTE—Data Terminal Equipment

DTG—Date-Time-Group

DTI—Digitized Technical Information

DTIC—Defense Technical Information Center

DTMF—Dual Tone Multiple Frequency

DTN—Data Transmission Network

DTP—Desktop Publishing

DTS—Data Terminal Set

DTS-C—DISN Transmission Services - CONUS

DTVTC—Desktop Video Teleconferencing

DUA—Directory User Agent

DUI—Data Use Identifier

DVD—1. Digital Versatile Disk
2. Digital Video Disk

DVD-R—Digital Versatile Disk - Recordable

DVD-RW—Digital Versatile Disk - Re-Writeable

DVD-ROM—Digital Versatile Disk - Read-Only Memory

DVI—1. Digital Video Interactive
2. Digital Video Instruction

DVOW—Digital Voice Orderwire

DVRS—Digital Voice Recorder System

DVS-G—DISN Video Services - Global

DX—Distance

E3—Electromagnetic Environmental Effects

EA—Electronic Attack

EAM—Emergency Action Message

EBCDIC—Extended Binary Coded Decimal Interchange Code

EC—1. Electronic Combat
2. Electronic Commerce
3. Echo Canceller

EC/EDI—Electronic Commerce/Electronic Data Interchange

ECAD—Electronic Computer-Aided Design

ECC—Error Correction Code

ECCM—Electronic Counter-Countermeasure

ECM—Electronic Countermeasure

ECO—Engineering Change Order

ECP—Engineering Change Proposal

ECR—Engineering Change Request

EDAC—Error Detection and Correction

EDI—Electronic Data Interchange

EDITS—Enhanced Digital Imagery Transmission System

EDMS—Electronic Document Management System

EDP—Electronic Data Processing

EDS—Electronic Data Systems

EEFI—Essential Elements of Friendly Information

EEI—1. Essential Elements of Information
2. External Environment Interface

EEPROM—Electrically Erasable Programmable Read-Only Memory

EF—Electronic Form

EFT—Electronic Funds Transfer

EFTO—Encrypt for Transmission Only

EGA—Enhanced Graphics Adapter

EGP—Extended Gateway Protocol

EHDC—EMP Hardened Dispersal Communications

EHF—Extremely High Frequency

EI—Engineering and Installation

EIA—Electronics Industry Association

EIS—Engineering Information System

ELF—Extremely Low Frequency

ELINT—Electronic Intelligence

EMC—1. Electromagnetic Compatibility
2. Emergency Message Change

EMCON—Emission Control

EMG—Enhanced Multinet Gateway

EMI—Electromagnetic Interference

EMP—Electromagnetic Pulse

EMR—Electromagnetic Radiation

EMRH—Electromagnetic Radiation Hazards

EMS—1. Electronic Message System
2. Extended Memory Specification

EMSEC—Emission Security

EMSS—Electronic Matrix Switching System

ENM—External Network Manager

ENTAC—Entrance National Agency Check

EO—Electro-Optics

EOD—End-of-Data

EOF—End-of-File

EP—Electronic Protection

EPBX—Electronic Private Branch Exchange

EPP—Endpoint Printer

EPROM—Erasable Programmable Read-Only Memory

ERM—Electronic Records Management

ERP—Effective Radiated Power

ES—End System

ESC—Emergency Status Code

ESD—Electrostatic Sensitive Device

ESDI—Enhanced System Device Interface

ESS—Electronic Switching System

ETADS—Enhanced Transmission Automated Data System

ETC—1. Earth Terminal Complex
2. Enhanced Terminal Communications

ETS—Electronic Transaction System

ETVS—Enhanced Terminal Voice Switch

EUCI—Endorsed for Unclassified Cryptographic Information

EW—Electronic Warfare

FAS—Functional Address Symbol

FAX—Facsimile

FBD—Formatted Binary Data

FBL—Functional Baseline

FCO—1. Frequency Controlled Oscillator
2. Facility Control Office

FCS—Full Communications Service

FDAd—Functional Data Administrator

FDDI—Fiber Distributed Data Interface

FEC—Forward Error Correction

FEP—Front End Processor

FIFO—First-In First-Out

FILO—First-In Last-Out

FIPS—Federal Information Processing Standard

FM—Frequency Modulation

FMHS—Formal Message Handling System

FMS—File Management System

FO—Fiber Optics

FOC—Final Operating Capability

FOIA—Freedom of Information Act

FORTEZZA—PCMCIA card with National Security Agency (NSA) encryption algorithm

FORTRAN—Formula Translator

FOT—Fiber Optics Transceiver

FPI—Functional Process Improvement

FRC—Federal Records Center

FS—File Server

FSA—Functional System Administrator

FSK—Frequency Shift Keying

FTP—File Transfer Protocol

FTS—1. Federal Telecommunications System
2. File Transfer System

GAN—Global Area Network

Gb—Gigabit

Gbyte—Gigabyte

GBS—Global Broadcast Service

GCC—Global Control Center

GCCS—Global Command and Control System

GCSS—Global Combat Support System

GEO—Geosynchronous Orbit

GEP—Ground Entry Point

GFE—Government Furnished Equipment

GFS—Government-Furnished Software

GHz—Gigahertz

GIF—Graphics Interchange Format

GIG—Global Information Grid

GII—Global Information Infrastructure

GILS—Government Information Locator Service

GIS—Geographical Information System

GM—Group Modem

GOCO—Government-Owned Contractor Operated

GOSIP—Government Open Systems Interconnection Profile

GOTS—Government-Off-The-Shelf

GPS—Global Positioning System

GRIB—Gridded Binary

GTS—Global Telecommunications Service

GUI—Graphical User Interface

GW—1. Gateway
2. Gigawatt

HAMPS—Host AUTODIN Message Processing System

HAR—Hardened Address Register

HAZCOM—Hazards Communication

HCI—Human Computer Interface

HCL—High-Capacity Links

HDA—Head-Drive Assembly

HDBS—Host Data-base System

HDLC—High Level Data-Link Control

HDTV—High Definition Television

HEMP—High Altitude Electromagnetic Pulse

HF—High Frequency

HF-ACP—High Frequency-Automated Communications Processor

HFRB—High Frequency Regional Broadcast

HFSSB—High Frequency Single Sideband

HICS—Hardened Intersite Cable System

HIPPI—High Performance Parallel Interface

HLI—Host Language Interface

HLL—High Level Language

HMA—High Memory Area

HMI—Human/Machine Interface

HNCA—Host Nation Connection Approval

HOL—High Order Language

HPA—High Power Amplifier

HPSC—High Performance Scientific Computer

HPW—High Performance Workstation

HSLC—High Speed Data Link Control

HSP—High Speed Printer

HSSI—High Speed Serial Interface Protocol

HTML—Hypertext Markup Language

HTTP—Hypertext Transfer Protocol

HUD—Heads Up Display

HUS—Hardened Unique Storage

HUSK—Hardened Unique Storage Key

HVPS—High Voltage Power Supply

HW—Hardware

HWRLP—Heavyweight, Rotatable, Log Periodic (antenna)

Hz—Hertz

I-CASE—Integrated Computer Aided Software Engineering

IA—Information Assurance

IAS—Immediate Access Storage

IAT—Installation and Acceptance Test

IBS—Intelligence Broadcast System

IC—1. Integrated Chip
2. Integrated Circuit
3. Interim Change

IC2—Integrated Command and Control

ICAD—Integrated Computer-Aided Design

ICAP—Integrated Communications Access Package

ICATS—Intermediate Capacity Automated Telecommunications System

ICB—Information Collection Budget

ICD—Installation Completion Date

ICDCS—Integrated Control, Display, and Communications Subsystem

ICI—Interactive Communications Interface

ICR—Information Collections and Reports

ICS—Integrated Communications Switch

ICU—Interface Control Unit

ICW—Interactive Courseware

ID—Initial Distribution

IDA—Initial Denial Authority

IDB—1. Integrated Data Base
2. Intelligence Data Base

IDEF—Integrated Definition

IDF—Intermediate Distribution Frame

IDN—Integrated Digital Network

IDS—Integrated Data System
Intrusion Detection System

IDTS—Integrated Digital Telecommunications System

IE—Information Engineering

IEC—Inter-Exchange Carriers

IEEE—Institute of Electrical and Electronics Engineers

IEMATS—Improved Emergency Message Automatic Transmission System

IEO—International Exchange Office

IF—Intermediate Frequency

IFF—Identification, Friend or Foe

IIW—Information-In-Warfare

ILS—Instrument Landing System

IM—Information Management

IMM—International Mail Manual

IMP—Interface Message Processor

IMS—Information Management System

IMU—Intermediate Message Unit

IMUX—Intelligent Multiplexor

IMWMPG—Information Management War and Mobilization Planning Group

INMARSAT—International Maritime Satellite Terminal

INP—Intelligent Network Processor

IO—Information Operation

IOC—Initial Operating Capability

IOP—Input/Output Processor

IP—Internet Protocol

IPC—Information Processing Center

IPE—Information Processing Equipment

IPMS—Information Processing Management System

IPO—Information Protection Operations

IPS—Information Processing System

IR—Infrared

IRK—Interswitch Rekeying Key

IRM—Information Resource Management

IRRM—Information Reports Requirements Manager

IS—1. Information System
2. Information Superiority

ISB—Independent Side Band

ISD—1. Information Systems Directive
2. Installation Start Date

ISDN—Integrated Services Digital Network

ISLMR—Intrinsically Safe Land Mobile Radio

ISOC—Internet Society

IST—Inter-Switch Trunk

IT—Information Technology

ITMRA—Information Technology Management Reform Act

ITN—Information Transfer Node

ITS—Information Transfer System

ITSEC—Information Technology Security

ITU—International Telecommunication Union

IVD—1. Interactive Video Disk
2. Interactive Video Display

IVSN—Initial Voice Switched Network

IW—Information Warfare

JBS—Joint Broadcast Services

JCCC—1. Joint Combat Camera Center
2. Joint Communications Control Center

JCEOI—Joint Communications-Electronics Operating Instruction

JCN—Joint Communications Network

JCSC—1. Joint Communications Satellite Center
2. Joint Communications Support Command

JCSE—Joint Communications Support Element

JDC—1. JUMPS Data Connectivity
2. Joint Deployment Community

JDD—Job Data Documentation

JETDS—Joint Electronic Type Designation System

JFMO—Joint Frequency Management Office

JINTACCS—Joint Interoperability of Tactical Command and Control Systems

JMAPS—Joint Message Analysis and Processing System

JMAS—Joint Mission Application Software

JRFL—Joint Restricted Frequency List

JRSC—Jam-Resistant Secure Communications

JRSC/SCP—Jam-Resistant Secure Communication/Secure Conferencing Project

JSIR—Joint Spectrum Interference Resolution

JTIDS—Joint Tactical Information Distribution System

JUDI—Joint Universal Data Interpreter

JWICS—Joint Worldwide Intelligence Communications System

JWID—Joint Warfare Interoperability Demonstration

KB—Kilobyte

kbps—Kilobits Per Second

kHz—Kilohertz

kVA—Kilovoltampere

KVD—Keyboard Visual Display

KVDT—Keyboard Video Display Terminal

KVDU—Keyboard Video Display Unit

KVG—Key Variable Generator

kW—Kilowatt

LAK—Look-Alike Disk

LAN—Local Area Network

LAN-OS—LAN Operating Systems

LAP—Link Access Procedure

LAP-B—Link Access Protocol-Balanced

LAPB—Link Access Procedure Balanced

LAP-D—Link Access Protocol D Channel

LAPD—Link Access Procedure for ISDN D Channels

LATA—Local Area Telecommunications Architecture

LAU—Line Amplifier Unit

LCA—Language Control Agent

LCATS—Large Capacity Automated Telecommunications System

LCD—Liquid Crystal Display

LD—Laser Diode

LDDI—Local Distributed Data Interface

LDM—1. Limited Distance Modem
2. Logical Data Model

LDMX—Local Digital Message Exchange

LDR—Low Data Rate

LEAD—Low-Cost Encryption/Authentication Device

LEASAT—Leased Satellite Communications System

LEC—Local Exchange Carrier

LED—Light-Emitting Diode

LEO—Low Earth Orbit

LF—Low Frequency

LHITA—Long Haul Information Transfer Architecture

LITA—Local Information Transfer Architecture

LITS—Local Information Transfer System

LMDS—Local Multipoint Distribution Service

LMR—Land Mobile Radio

LMST—Lightweight Multiband Satellite Terminal

LNA—Low Noise Amplifier

LO—Local Oscillator

LOC—Line of Code

LORAN—Long-Range Aid to Navigation

LOS—Line-of-Sight

LP—Laser Printer

LPA—Low Power Amplifier

LPC—Linear Predictive Coding

LPD—Low Probability of Detection

LPM—Lines Per Minute

LPU—1. Line Printer Unit
2. Link Processing Unit

LRA—Local Reproduction Authorized

LRM—Low Rate Multiplexer

LRR—Long-Range Radar

LRU—Line Replaceable Unit

LSB—1. Least Significant Bit
2. Lower Sideband

LSC—LAN Software Contract

LSD—Least Significant Digit

LSDA—Local Directory System Agent

LSTDM—Low Speed Time Division Multiplex

LSU—1. Line Switch Unit
2. Line Sharing Unit

LTU—Line Terminating Unit

LUF—Lowest Useable Frequency

MAN—Metropolitan Area Network

MAO—Mail Address Only

MARS—Military Affiliated Radio System

MART—Modular Automated Remote Terminal

MAST—MILSTAR Advanced Satellite Terminal

Mb—Megabit

MB—Megabyte

MBA—Multi-Beam Antenna

MBd—Megabaud

MBMMR—Multi-Band Multi-Mode Radio

Mbps—Megabits per second

MCCR—Mission Critical Computer Resources

MCE—Modular Control Equipment

MCEB—Military Communications-Electronics Board

MCS—Message Conversion System

MDB—Main Data Bus

MDC—Message Distribution Center

MDF—Main Distribution Frame

MDR—Medium Data Rate

MDT—Message Distribution Terminal

MECL—Minimum Essential Circuit Listing

MEECN—Minimum Essential Emergency Communications Network

MEITS—Mission Essential/Effective Information Transmission System

MF—Medium Frequency

MH—Message Host

MHF—Medium High Frequency

MHS—Message Handling System

MHz—Megahertz

MICK—Mobility Initial Communications Kit

MIB—Management Information Base

MIF—Multiple Interface

MIJI—Meaconing, Interference, Jamming, and Intrusion

MIL-HDBK—Military Handbook

MIL-STD—Military Standard

MILNET—Military Network

MILSAT—Military Satellite

MILSATCOM—Military Satellite Communications

MILSTAMP—Military Standard Transportation and Movement Procedures

MILSTAR—Military Strategic and Tactical Relay Satellite

MINSL—Minimum Security Level

MIPR—Military Interservice Procurement Request

MIPS—Millions of Instructions Per Second

MIRA—Microprocessor Integrated Reliable Architecture

MIRS—Management Information and Research System

MIS—Management Information System

MISSI—Multi-Level Information System Security Initiative

MIST—Meteorological Information Standard Terminal

MLA—Mail List Agent

MLP—Multi-Line Phone

MLPP—Multilevel Precedence and Preemption

MLS—1. Microwave Landing System
2. Multi-Level Security

MMI—Man-Machine Interface

MMLS—Mobile Microwave Landing System

MMRT—Modified Miniature Receive Terminal

MNCS—Master Net Control Station

MODEM—Modulator/Demodulator

MOS—Monolithic Oxide Silicon

MPC—Multimedia Personal Computer

MPD—Master Power Distributor
Message Preparation Directory

MPDT—Message Processing Data Terminal

MPL—1. Multischedule Private Line
2. Master Publication Library

MPOE—Minimum Point of Entry

MPU—Message Processing Unit

MRA—Minimum Receive Antenna

MRK—Manual Remote Keying

MRT—Miniature Receive Terminal

MSB—Most Significant Bit

MSD—Most Significant Digit

msec—Millisecond

MSEP—Maintenance Standardization and Evaluation Program

MSL—Master Station Log

MS2—Message Switching and Mail Service

MSU—Main Storage Unit

MTA—Message Transfer Agent

MTF—1. Message Text Formatting
2. Modulation Transfer Function

MTS—Message Transfer System

MUF—Maximum Usable Frequency

MUI—Management User Interface

MUX—Multiplex(er)

MVS—Multiple Virtual Storage

MW—1. Megawatt
2. Microwave

MWS—Management Work Station

NACAM—National COMSEC Advisory Memorandum

NACSI—National COMSEC Instruction

NAVAIDS—Navigational Aids

NA—Network Administration

NARA—National Archives and Records Administration

NAT—Network Address Translator

NB—Narrowband

NCC—Network Control Center

NCS—Network Control Station

NDS—1. Network Directory Service
2. Non-Developmental Software

NES—Network Encryption Standard

NFE—Network Front End

NFS—Network File System

NGCR—Next Generation Computer Resources

NIC—Network Information Center

NID—Network-Inward Dialing

NIDMO—Network-Inward Dialing, Manual Out

NII—National Information Infrastructure

NIMA—National Imagery and Mapping Agency

NIPRNET—Non-Secure Internet Protocol Router Network

NIS—Network Information Services

NIST—National Institute for Standards and Technology

N-ISDN—Narrowband-Integrated Services Digital Network

NM—Network Management

NMO—Network Management Office

NMS—Network Management System

NNTP—Network News Transfer Protocol

NOSC—Network Operations and Security Center

NOD—Network Outward Dialing

NOS—Network Operating System

NSAD—Network Security Architecture and Design

NSO—Network Security Officer

NSP—Network Service Protocol

NT—Net Terminal

NTC—Network Terminal Concentrator

NTIS—National Technical Information Service

NTISSP—National Telecommunications and Information Service Policy

NTIU—Network Terminal Interface Unit

NTP—Network Time Protocol

NVM—Nonvolatile Memory

NVRAM—Nonvolatile Ram

NVT—Network Virtual Terminal

OA—Office Automation

OAS—Office Automation System

OC—Optical Carrier

OCI—Offensive Counterinformation

OCR—Optical Character Reader

ODI—Open Datalink Interface

ODT—Optical Digital Technologies

OF—Optional Form

OIS—Office Information System

OLTP—On-Line Transaction Processor

OMR—Optical Mark Reader

ONC—Open Network Computing

O/PTN—Operationalize and Professionalize the Network

OPX—Off Premise Extension

OS—Operating System

OSE—Open System Environment

OSI—Open System Interconnection

OSI-MHS—Open System Interconnect—Message Handling System

OTH-B—Over-the-Horizon Backscatter

OTH-R—Over-the-Horizon Radar

OTI—Office of Technical Integration

OTDR—Optical Time Domain Reflectometer

OTS—Off-the-Shelf

OTSS—Operational Telecommunications Switching System

OW—Order Wire

PA—Privacy Act

PABX—Private Automatic Branch Exchange

PAD—1. Packet Assembler/Disassembler
2. Power Attenuation Device

PAL—1. Program Assembler Language
2. Parcel Airlift
3. Phase Alternate Line

PAP—Password Authentication Protocol

PAX—Private Automatic Exchange

PB—1. Postal Bulletin
2. Publishing Bulletin

PBX—Private Branch Exchange

PC—1. Personal Computer
2. Postal Clerk

PCB—Printed Circuit Board

PCCIE—Power Conditioning and Continuation Interfacing Equipment

PCI—Peripheral Component Interface

PCM—Pulse-Code Modulation

PCMCIA—Personal Computer Memory Card International Association

PCMT—Personal Computer Message Terminal

PC/NFS—Personal Computer/Network File System

PCS—Personal Communications System

PCU—Power Converter Unit

PD—Pulse Duration

PDC—Program Designator Code

PDH—Plesiochronous Digital Hierarchy

PDI—1. Picture Description Language
2. Power Data Interface

PDM—Publishing Distribution Manager

PDO—Publishing Distribution Office/Officer

PDOS—Publishing Distribution Office System

PDL—Publication Distribution Library

PDP—1. Procedure Definition Processor
2. Programmed Data Processor

PDS—Publishing Distribution System

PDU—1. Power Distribution Unit
2. Protocol Data Unit

PE—Phase Encoded

PEP—Peak Envelope Power

PGWS—Primary Groupware Server

PIA—Peripheral Interface Adapter

PIF—Productivity Investment Fund

PIM—Procedural Instruction Message

PING—Packet Internet Gopher

PITN—Primary Information Transfer Nodes

PKI—Public Key Infrastructure

PLA—Plain Language Address

PLL—Phase Locked Loop

PLN—Private Line Network

PLO—Phased Locked Oscillator

PLP—1. Packet Layer Protocol
2. Procedural Language Processor

PM—Phase Modulation

PMD—Program Management Directive

PMI—Preventive Maintenance Inspection

PnP—Plug-and-Play

POP—Post Office Protocol

POSE—Picture Oriented Software Engineering

POSI—Portable Operating System Interface

POSIX—Portable Operating System Interface for Computer Environments

POTS—Purchase of Telecommunication Service

PPM—1. Pages Per Minute
2. Pulse Position Modulation

PPP—Point-to-Point Protocol

PPS—1. Packets Per Second

2. Pulse Per Second

PRISM—Programmable-Reconfigurable-Integrated-Switch and Multiplex

PROM—Programmable Read-Only Memory

PRR—Pulse Repetition Rate

PRF—Pulse Recurrence Frequency

PSCF—Primary System Control Facility

PSN—Packet Switching Node

PSS/CCTV—Perimeter Surveillance System/Closed Circuit Television

PSTN—1. Packet Switched Telecommunications Network
2. Public Switched Telephone Network

PT—Printer-Only Terminal

PTF—Patch and Test Facility

PTM—Packet Transfer Mode

PTSN—Public Telephone Switching Network

PVC—Permanent Virtual Circuit

PWCS—Personal Wireless Communications System

PWDS—Protected Wire Distribution System

QOS—Quality of Service

QRC—Quick Reaction Capability

QRCT—Quick Reaction Capability Terminal

QRP—1. Query and Reporting Processor
2. Quick Reaction Package

QRSA—Quick Reaction Satellite Antenna

RACE—Rapid Automatic Cryptographic Equipment

RADAR—Radio Detection and Ranging

RADAY—Radio Day

RADHAZ—Radiation Hazard

RAIDS—Real-Time AUTODIN Interface Distribution System

RAM—Random Access Memory

RAMS—Reprographics Automated Management System

RAPCON—Radar Approach Control

RATT—Radio Teletype

RATTS—Regional Automated Tape Transfer System

RC—Records Custodian

RCC—Regional Control Center

RCS—Report Control Symbol

RCU—Remote Control Unit

RCVR—Receiver

RDA—Remote Data Base Access

RDB—Relational Data Base

RDBME—Relational Data Base Management Environment

RDBMS—Relational Data Base Management System

RDD—Required Delivery Date

RDL—Remote Data Link

RDM—Relational Data Base Machine

RDMS—Relational Data Base Management System

RDPC—Regional Data Processing Center

RDT—Remote Digital Terminal

REM—Recognition Memory

RF—Radio Frequency

RFA—Radio Frequency Authorization

RFE—Receiver Front End

RFI—Radio Frequency Interference

RFO—Radio Frequency Oscillator

RFS—1. Remote File System
2. Request for Service

RGB—Red/Green/Blue

RI—Routing Indicator

RICK—Rapid Initial Communications Kit

RIMS—Records Information Management System

RIP—Routing Information Protocol

RJE—Remote Job Entry

RJETS—Remote Job Entry Terminal System

RLP—Remote Line Printer

RM—Records Manager

RN—Relay Node

RNP—1. Remote Network Printer
2. Remote Network Processor

RNR—Receive Not Ready

RO—Receive Only

ROSC—Regional Operations and Security Center

ROD—Required Operational Date

ROM—Read-Only Memory

ROP—Receive-Only Printer

RP—1. Recurring Periodical
2. Restoration Priority

RPC—1. Regional Processing Center
2. Remote Processing Computer

RPL—Restoration Priority List

RPPO—Regional Printing Procurement Office

RSI—1. Remote Symbiotic Interface
2. Remote Status Indicator

RSN—RED Switch Network

RST—Remote Switching Terminal

R/T—Receiver/Transmitter

RTCP—Real-Time Communications Protocol

RTE—Remote Terminal Emulator

RTOS—Real-Time Operating System

RSU—Remote Switching Unit

RW—Read/Write

RX—Receive

RZ—Return-to-Zero

SA—1. Security Assistance
2. System Administrator

SADL—Situational Awareness Data Link

SAM—Space Available Mail

SAMM—Security Assistance Management Manual

SAN—1. System Advisory Notice
2. System Area Network

SAR—1. Subaccount Representative

2. Service Activation Request
3. Satellite Access Request

SARSAT—Search and Rescue Satellite-Aided Tracking

SATCOM—Satellite Communications

SBI—Special Background Investigation

SBIT—Standard Base Infrastructure Template

SBLC—Standard Base-Level Computer

SBLCC—Standard Base-Level Communications-Computer

SC—1. Systems Code
2. Communications and Information Directorate

SCCB—Software Configuration Control Board

SCCC—Satellite Communications Control Center

SCCE—Satellite Configuration Control Element

SCI—1. Special Compartmented Information
2. System Control Interface

SCINET—Sensitive Compartmented Information Network

SCIS—Survivable Communications Integration System

SCL—Site Concurrence Letter

SCM—Scramble Code Multiplexer

SCN—1. Satellite Communications Node
2. System Change Notice

SCOTT—Single Channel Objective Tactical Terminal

SCSC—Small Computer Support Center

SCSI—Small Computer System Interface

SCT—1. Satellite Communications Terminal
2. Single Channel Transponder
3. Secure Cellular Telephone

SCTC—Small Computer Technical Center

SDA—Software Design Activity

SDE—Source Data Entry

SDH—Synchronous Digital Hierarchy

SDIF—SGML Document Interchange Format

SDL—Software Development Library

SDN—System Development Notification

SDNRIU—Secure Digital Net Radio Interface Unit

SDNS—Secure Data Network System

SDP—Software Development Plan

SDS—Space Defense System

SDT—Software Development Tool

SE—1. Software Engineering
2. Software Evaluator

SEON—Solar Electro-Optical Network

SERL—System Engineering Reference Library

SETA—System Engineering and Technical Assistance

SF—Standard Form (*used on designated forms*)

SFS—Shared File System

SGDB—Satellite Global Data Base

SGML—Standard Generalized Markup Language

SHF—Super High Frequency

SHR—Self Healing Ring

SHTTP—Secure Hypertext Transfer Protocol

SI—Special Intelligence

SIDS—1. Satellite Information Dissemination System
2. Secondary Imagery Dissemination System

SIGINT—Signals Intelligence

SII—System Internal Interface

SIMM—Single In-line Memory Module

SINCGARS—Single Channel Ground and Airborne Radio System

SIP—Serial Interface Port

SIPRNet—Secret Internet Protocol (IP) Router Network

SIPTO—Standard Installation Practice Technical Order

SITN—Secondary Information Transfer Nodes

SIU—Storage Interface Unit

SL—Sensitivity Level

SLC—Subscriber Line Concentrator

SLFCS—Survivable Low Frequency Communications System

SLIP—Serial Line Internet Protocol

SLP—Single Line Phone

SMP—Symmetric Multiprocessing

SMR—Specialized Mobile Radio

SMSC—Standard Multi-User Small Computer

SMSCRC—Standard Multi-User Small Computer Requirements Contract

SMT—Surface Mail Transport

SMTP—1. Simple Mail Transfer Protocol
2. Simple Message Transfer Protocol

S/N—Signal-to-Noise Ratio

SN—Serial Number

SNA—Systems Network Architecture

SNI—1. Standard Network Interface
2. Subscribers Network Interfaces
3. System Network Interconnect

SNMP—Simple Network Management Protocol

SOCR—Stand-Alone Optical Character Reader

SOCS—Strategic Operations Communications System

SON—Statement of Need

SONET—Synchronous Optical Network

SOP—Standard Operating Procedure

SOR—Statement of Requirement

SORD—System Operational Requirements Document

SPA—Software Process Assessment

SPI—System Programming Interface

SPIN—Software Process Improvement Network

SPIP—Software Process Improvement Program

SPM—System Programmer's Manual

SPN—Shared Processing Network

SQL—Structured Query Language

SRD—1. Standard Reporting Designator
2. Systems Requirement Document

SRIP—Software Reuse Implementation Plan

SSA—Software Support Activity

SSB—Single Sideband

SSI—Signal-Strength Indicator

SSP—System Support Processor

SSUPS—Solid State Uninterruptible Power Supply

S&T—Science and Technology

ST—Subscriber Terminal

STAMPS—Stand-Alone Message Processing System

STANAG—Standardization Agreement

STATMUX—Statistical Multiplexer

STDM—Synchronous Time Division Multiplexing

STE—Secure Terminal Equipment

STEM—Systems Telecommunications Engineering Manager

STEM-B—Systems Telecommunications Engineering Manager-Base Level

STEM-C—Systems Telecommunications Engineering Manager-Command Level

STEM-J—Systems Telecommunications Engineering Manager-Joint

STEM-R—Systems Telecommunications Engineering Manager-ANG Regional

STEM-TM—Systems Telecommunications Engineering Manager-Technical Manager

STEP—Standardized Tactical Entry Point

STID—Standard Identification

STINFO—Science and Technology Information

STM—Synchronous Transfer Mode

STP—Shielded Twisted Pair

STS—Synchronous Transport Signal

STT—Satellite Tactical Terminal

STU—Secure Telephone Unit

STU-III—Secure Telephone Unit-III

STV—Surveillance Television

SUM—Software User’s Manual

SVC—Switched Virtual Circuit

SVGA—Super Video Graphics Array

SVS—Switched Voice Service

SW—Software

SWR—Standing Wave Ratio

SYS—System

SYSGEN—System Generation

TA—Technical Architecture

TAC—1. Terminal Access Controller
2. Tactical

TACAN—Tactical Air Navigation System

TACTERM—Tactical Terminal

TADIL—Tactical Digital Information Link

TAFIM—Technical Architecture Framework for Information Management

TAISS—Telecommunications and Automated Information System Security

TASO—Terminal Area Security Officer

TBVC—Terminal Box, Video Cable

TCA—Tactical Communications Architecture

TCC—Telecommunications Center

TCF—Technical Control Facility

TCM—Time Compression Multiplexing

TCMD—Transportation Control and Movement Document

TCO—1. Telecommunications Certification Office/Officer
2. Telecommunications Control Office
3. Telephone Control Officer

TCP—Transmission Control Protocol

TCP/IP—Transmission Control Protocol/Internet Protocol

TDC—Theater Deployable Communications

TDF—Tactical Digital Facsimile

TDM—Time-Division Multiplexer

TDMA—Time-Division Multiple Access

TDR—Time Domain Reflectometer

T&E—Test and Evaluation

TED—Trunk Encryption Device

TELEFAX—Telecommunications Facsimile

TELNET—Telecommunications Network

TFS—Time Frequency Standard

TFTP—Trivial File Transfer Protocol

THz—Terahertz

TIA—Transmission Interface Adapter

TIFF—Tag Image File Format

TIP—Terminal Interface Processor

TIR—Technical Integration Repository

TITN—Tertiary Information Transfer Nodes

TLMR—Trunked Land Mobile Radio

TMAP—Telecommunications Monitoring and Assessment Program

TMUX—Terminal Multiplexer

TMS—Telecommunications Management System

TMSC—Transportation Management Service Center

TCP—Transmission Control Protocol

TO—Technical Order

TOF—Time of File

TOR—Time of Receipt

TOT—Time of Transmission

TP—Transaction Processor

TRANSEC—Transmission Security

TRI-TAC—Tri-Service Tactical Communications (Program)

TRC—Technical Reference Code

TRM—Technical Reference Model

TROPO—Tropospheric Scatter

T&S—Timing and Synchronization

TSO—Telecommunications Service Order

TSP—Telecommunications Service Priority

TSR—Telecommunications Service Request

TSP—Time Synchronization Protocol

TSSP—Tactical Satellite Signal Processor

TTISSMM—Transit Time Information Standard System for Military Mail

TWT—Traveling Wave Tube

TX—Transmit

UA—User Agent

UAS—User Application Software

U/C—Upconverter

UCI—User Computer Interface

UDC—1. Unit Descriptor Code
2. Universal Downconverter

UDS—Universal Data System

UDT—Unstructured Data Transfer

UEF—User Exchange Format

UHF—Ultra High Frequency

UI—1. Unit of Issue
2. User Interface

UIC—Unit Identification Code

UIDL—User Interface Definition Language

UIL—User Interface Language

UKB—Universal Keyboard

ULANA—Unified Local Area Network Architecture

ULF—Ultra Low Frequency

UM—Universal Modem

UMB—Upper Memory Block

UMS—Universal Modem System

UPS—Uninterruptible Power Supply

URDB—User Requirements Data Base

URL—Uniform Resource Locator

USB—1. Universal Serial Bus
2. Upper Sideband

USHR—Unidirectional Self Healing Ring

USMTF—United States Message Text Formatting

UT—Universal Time
User Terminal

UTC—Unit Type Code

UTP—Unshielded Twisted Pair

UTS—Universal Terminal System

V—Volts

VA—Volt-Ampere

VAC—Voltage Alternating Current

VAN—Value Added Network

VAPI—Virtual Application Programming Interface

VAX—Virtual Address Extension

VBR—Variable Bit Rate

VC—Virtual Circuit

VCI—Virtual Channel Identification

VCO—Voltage Controlled Oscillator

VCSS—Voice Communications Switching System

VDI—Virtual Device Interface

VDM—Virtual Device Metafile

VDT—Video Display Terminal

VDU—Visual Display Unit

VF—Voice Frequency

VGA—Video Graphics Adapter

VHF—Very High Frequency

VHS—Video Handling System

VHSIC—Very High Speed Integrated Circuit

VI—Visual Information

VIDOC—VI Documentation

VIEP—Visual Information Equipment Plan

VIP—Visual Information Processor

VIRIN—Visual Information Record Identification Number

VISC—Visual Information Support Center

VITAB—Visual Information Technology Advisory Board

VLAN—Virtual Local Area Network

VLF—Very Low Frequency

VLSI—Very Large Scale Integration

VME—Virtual Memory Expansion

VMF—Variable Message Format

VMM—Virtual Memory Manager

VMS—Virtual Memory System

VNMC—Video Network Management Center

VOCODER—Voice Coder (Encoder-Decoder)

VOIP—Voice Over Internet Protocol

VOM—Volt-Ohmmeter

VOR—VHF Omnidirectional Range

VORTAC—VHF Omni-Range Tactical Air Navigation

VPI—Virtual Path Identification

VPN—Virtual Private Network

VRML—Virtual Reality Modeling Language

VSAT—Very Small Aperture Terminal

VSS—1. Video Storage System
2. Voice Switching System

VSWR—Voltage Standing Wave Ratio

VT—Virtual Terminal

VTC—Video Teleconferencing

VTCN—Video Teleconference Communication Network

VTE—Video Teleconferencing Equipment

VTP—Virtual Terminal Protocol

VTU—Video Teleconferencing Unit

WAN—Wide Area Network

WADS—Wide Area Data Service

WATS—Wide Area Telecommunications Service

WBS—Wireless Broadband System

WCCS—Wing Command and Control System

WDM—Wavelength Division Multiplexing

WICP—Wing Initial Communications Package

WICS—Wing Integrated Communications System

WICU—Weather Intercept Control Unit

WGM—Workgroup Manager

WLAN—Wireless Local Area Network

WOM—Write-Only Memory

WORM—Write-Once, Read-Many

WP—Word Processor

WPM—Words Per Minute

WWW—World Wide Web

XAP-TP—X/Open API-Transaction Processing

XCDR—X/Open CD-ROM

XDR—External Data Representation

XDS—X/Open Directory Service

XLFD—X/Logical Font Description

XMOG—X/Open Managed Object Guide

XMP—X/Open Management Protocol

XMPP—X/Open Management Protocol Profiles

XML—Extended Markup Language

XMS—Extended Memory Specification

XNFS—X/Open Network File System

Y2K—Year 2000

Z—ZULU Time

ZCS—Zero Code Suppression

ZIF—Zero Insertion Force

Zo—Characteristic Impedance

Terms

Acceptance—(of a communications and information facility/system) —Indicates a facility or system generally meets technical and performance standards but may have minor exceptions that do not keep the facility from meeting operational and security requirements.

Acceptance Inspection—The final inspection to determine if a facility or system meets the specified technical and performance standards. It is held immediately after facility and software testing, and is the basis for commissioning or accepting the C4 system.

Access—1. A user's ability to communicate with (input to or receive output from) a system or to have entry to a specified area. 2. Allowing individuals to review or receive copies of their records.

Access lines—Two-wire or four-wire circuits that allow user equipment to gain access to the network.

Accuracy—Free from error. Accuracy denotes the absolute quality of computed results. In contrast, precision refers to the degree to which computed results reflect theoretical values.

Acquisition—In satellite communications, the process of locking tracking equipment on a signal from a communications satellite (referred to as "acquiring the satellite").

Adaptive Communications—A communications system, or part thereof, that automatically uses feedback information obtained from the system itself or from the signals carried by the system to modify dynamically one or more of the system operational parameters to improve system performance or to resist degradation.

Adaptive Radio—A radio that (a) monitors its own performance, (b) monitors the path quality through sounding or polling, (c) varies operating parameters, such as frequency, power, or data rate, and (d) uses closed-loop action to optimize its performance by automatically selecting frequencies or channels.

Adjacent Channel—In communications, the next channel or the one in close proximity, either physically or electrically, to the one in use.

Adopted Form—DoD does not prescribe these forms and their use by the military departments is optional. DoD develops these forms when two or more military departments or DoD agencies have a common requirement. Within Air Force, however, the office of primary responsibility prescribes them in an Air Force standard or specialized publication. They are shown as prescribed, not adopted, in that publication.

Advanced Research Projects Agency Network (ARPANet)—The precursor to the Internet. Developed in the late 1960's and early 1970's by the DoD as an experiment in wide-area networking that would survive a nuclear war.

Automated Data Processing (ADP)—That branch of science and technology concerned with methods and techniques relating to data processing largely performed by automatic means.

Agency Disclosure Notice (ADN)—A statement used for public information collections. It is put on the instrument of collection as close to the current Office of Management and Budget (OMB) control number as practicable. It is the agency's disclosure of the estimated average burden hours per response and a request that the public direct any comments concerning the accuracy of this burden estimate and any suggestions for reducing this burden to the agency and to OMB's Office of Information and Regulatory Affairs.

Air Force C4 Systems Architectures—A multi-volume family of documents that provides guidance on goals, objectives, and strategies for planning future C4 systems.

Air Force Corporate Data Dictionary (AFCDD)—A composite program consisting of the Air Force Data Dictionary, Computer Systems Authorization Directory, Air Force Information Resources Dictionary System, and Model Library.

Air Force Electronic Publications Library (AFEPL)—The compact disk-read only memory based repository of electronic publications and forms.

Air Force Equipment Management System (AFEMS)—The official inventory and account for communications, electronics, and other equipment centrally managed by Headquarters Air Force Materiel Command.

Air Force Information Architecture—A framework that depicts the relationships of elements involved in information management within an organization. Within the Air Force, it is used to provide a blueprint for developing specific plans and actions in the planning, control, and management of Air Force information.

Air Force Information Resources Dictionary System (AFIRDS)—A software tool used as a data dictionary for management of metadata (data about data). It supports research and maintenance of existing data elements and is used to create new elements using the DoD standardization guidelines.

Air Force Integrated Telecommunications Network (AFNET)—A dedicated, high speed, wideband information transport system combining common user, and command, control, communications, and computer circuits into a single, integrated, centrally managed network. AFNET supports voice circuits and data circuits with rates from 1.2 kbps to 45 Mbps.

Air Force Internet (AFIN)—The standard, unclassified Internet protocol and connectionless network service wide area network touching every major USAF installation worldwide, and is part of the Global Internet. Applications include computer-aided design/manufacturing, multimedia mail, image processing, and graphics applications.

Air Force Publication Distribution Library (AFPDL)—The electronic bulletin board system used for the dissemination of all Air Force electronic-based publications and forms.

Air Force Satellite Communications (AFSATCOM) System—An ultra high frequency (UHF) satellite communications system that provides reliable UHF, two-way command and control communications between the National Command Authority and globally deployed nuclear forces. The system is composed of satellites of the United States Navy's Fleet Satellite Communications System, the Air Force's Satellite Data System, UHF single-channel transponders integrated into Defense Satellite Communications System III satellites, ground, and airborne terminals.

Algorithm—A finite set of well-defined rules for the solution of a problem in a finite number of steps.

Algorithmic Language (ALGOL)—A high-level computer language used to express problem-solving formulas for machine solution.

Allied Long Lines Agency (ALLA)—A multinational organization organized under the North Atlantic Treaty Organization (NATO) to process and coordinate leased long-lines circuit orders of NATO, Supreme Headquarters Allied Powers Europe, and national military forces residing in the NATO area.

Allocated Circuit—A circuit designated for use (whether "common user" or "dedicated").

Alternate Route (Altroute)—A secondary communications path used to reach a destination if the primary path is unavailable.

Alternate Use—An arrangement that permits the use of a circuit for different types of transmission such as voice, data, facsimile, magnetic tape, etc. Normally, only one type of operation is possible at any one time (alternate use), although simultaneous use is possible in some instances. The use of a circuit exclusively for voice communications, even though both secure and nonsecure voice conversations are passed over the circuit, is not considered alternate use.

Alternate Voice Data (AVD)—or Alternate Voice Record (AVR) Interchangeable terms that describe the alternate use of circuits when one use is for voice (non-record) conversations and the other use is for record communications. Transfer arrangements and conditioning equipment are normally required for alternate use. When a circuit is used exclusively for voice, even though the voice conversations may appear as data on the transmission path between the end terminals, the circuit is not considered as an alternate voice data or alternate voice record circuit.

Amendment—The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

American National Standard (ANS)—Any standard, supported by a national consensus, developed, approved, and cleared through the American National Standard Institute.

American National Standards Institute (ANSI)—American national standards for information systems are issued periodically by ANSI. Industry standards that the Air Force has adopted are published in the *DoD Index of Specifications and Standards*.

American Standard Code for Information Interchange (ASCII)—1. The standard representation of numbers and letters by computers other than IBM (see also Extended Binary Coded Decimal Interchange Code). 2. The coded character set used for the general interchange of information among information processing systems and associated equipment. A standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), used for information interchange among data processing systems, data communication systems, and associated equipment. (a) ASCII Character Set: The ASCII 8-bit character set. It consists of the first 128 (0-127) characters of the ANSI character set. (b) ASCII Text A subset of the ASCII, common to all computer devices, consisting principally of the printable characters.

Amplifier—In electronics, a normally unidirectional device that increases the power or amplitude of a (input) signal.

Amplitude Distortion—Distortion occurring in an amplifier or other electronic device when the amplitude of the output is not a linear function of the input amplitude under specified conditions.

Amplitude Equalizer—A corrective network that is designed to make the amplitude characteristics of a circuit or system substantially equal over a desired frequency range.

Amplitude Modulation (AM)—A form of modulation in which the amplitude of a carrier wave is varied in accordance with the instantaneous value of the modulating signal.

Analog Data—Data represented as a physical quantity that is considered to be continuously variable and whose magnitude is made directly proportional to the data or to a suitable function of the data.

Analog—1. A transmission mode in which information is encoded on a carrier wave by a continuously variable current or voltage level. 2. Pertaining to a device that measures a continuous variable (such as temperature on a thermometer) instead of indiscrete numbers.

Anchor—A synonym for hyperlink. (A link in a given document to information within another document)

Anisynchronous—Pertaining to transmission in which the time interval separating any two significant instants in sequential signals is not necessarily related to the time interval separating any other two significant instants. **NOTE:** Isochronous and Anisynchronous are characteristics, while Synchronous and Asynchronous are relationships.

Anomalistic Period—In satellite communications, the time interval between two successive passages of a satellite through its apogee.

Anomalous Propagation—In radio communications, abnormal propagation due to discontinuities in the atmosphere and resulting, in many instances, in the reception of signals well beyond their normal range.

Answerback Data—A signal or tone sent by the receiving business machine or data set to the sending station for identification or to indicate it is ready to receive transmission.

Antenna—In radio communications, a device that converts a radio frequency signal into a corresponding electromagnetic wave or vice versa.

Anthropomorphic Factors—Human body measurements involved with the design requirements of a system when the system is dependent upon humans for operation. Thus, such factors as weight, height, arm reach, hand size, and so forth, become critical when designing operator stations, control panels, aircraft cockpits, and so forth.

Aperiodic Antenna—An antenna designed to have an approximately constant input impedance over a wide range of frequencies.

Aperture Antenna—A microwave radio antenna employing a horn for a feed and reflector.

Aperture—1. In computing, a part of a mask that permits retention of the corresponding portions of data. 2. In radio communications, the open end of a horn antenna.

Apogee—The point in its orbit at which a satellite is at its maximum distance from the Earth.

Application (Program)—A computer program used for a particular kind of work, such as word processing or data base management. The term is commonly used interchangeably with “program.”

Application (Software) Architecture—A framework for developing a software environment responsive to user information requirements.

Application Model—A term used to describe those functions of an organization that can be supported or automated through information technology (IT). Used for grouping or clustering functions into applications. It provides the application developers’ views of the IT architecture.

Application Platform—The collection of hardware and software components that provide the services used by support and mission-specific software applications.

Application Portability Profile—The structure that integrates federal, national, international, and other specifications to provide the functionality necessary to accommodate the broad range of federal information technology requirements.

Application—A computer program that performs a specific function, such word processing, electronic mail, data base management, etc. A commonly used term interchangeable with program.

Application Program Interface (API)—1. The interface between the application software and the application platform, across which all services are provided. The API is primarily in support of application portability, but system and application interoperability are also supported by a communications API. 2. A set of formalized software calls and routines that can be referenced by an application program to access underlying network services.

Application Software—Software that manipulates data, creates reports, performs calculations, and so forth. Word processing, data base, graphics, and spreadsheet packages are examples of applications software.

Application Window—In computing, the window containing the work area and menu bar for an application. An application window may contain multiple document windows.

Appraisal—The process of determining the value and thus the final disposition of a record, making it either temporary or permanent. The National Archives and Records Administration is the only Federal agency with the authority to appraise government records.

Architecture—There are many different types of architectures, each with its own definition. The following are the DoD-approved definitions. (a) General Definition: A framework or structure that portrays relationships among all the elements of the subject force, subject, or activity. (b) The standard definitions for Operational, Systems, and Technical Architecture: Operational Architecture. A description of the tasks, operational elements, and information flows required to accomplish or support a war-fighting function. Systems Architecture. A description, including graphics, of the systems and interconnections providing for or supporting a war-fighting function. Technical Architecture. A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements of a system, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Arrester—In telecommunications, an electro-mechanical device that protects equipment and circuits from voltage or current surges produced by lightning or an electromagnetic pulse. Synonym: Surge Suppressor.

Artificial Intelligence—The capability of a computer to perform functions that are normally attributed to human intelligence, such as learning, adapting, recognizing, classifying, reasoning, self-correction, and improvement.

Artificial Intelligence Languages—Artificial intelligence languages are a subfield within computer science concerned with developing a technology to enable computers to solve problems (or assist humans to solve problems). They use explicit representations of knowledge and reasoning methods employing that knowledge.

Assembler—A computer program that translates symbolic codes into machine instructions, item for item.

Assembly—An item of equipment forming a portion of an end item of (communications) equipment and which item can be provisioned and replaced as an entity. An assembly normally incorporates replaceable parts or groups of parts.

Assigned Frequency—The frequency of the center of the radiated bandwidth.

Asynchronous Operation—An operation that occurs without a regular or predictable time relationship to a specified event; (e.g., the calling of an error diagnostic routine that may receive control at any time during the execution of a computer program). Also, a sequence of operations in which operations are executed but out-of-time coincidence with any event.

Asynchronous System—A system employing start and stop elements for individual synchronization of each character information, or each word or block. The gaps between characters or words may be of variable length. (Synonym: Start-Stop System.)

Asynchronous Transfer Mode (ATM)—A key broadband switching and transport technology that supports high-speed data, video, imaging, and voice applications as well as combinations of these in multimedia applications. ATM can do this as a multi-service platform using a single network rather than requiring separate networks specific to a service. It can send digitized information at more than 45,000 times the speed available on typical telephone lines. ATM is not an asynchronous transmission technique; transfer mode refers to the switching and multiplexing process.

Asynchronous Transmission—1. A form of discontinuous data transmission that employs start and stop bits to signify the beginning and end of characters. Compare with Synchronous Transmission. 2. A transmission process such that between any two significant instants in the same group (in data transmission, this group is a block or a character) there is always an integral number of unit intervals. Between two significant instants located in different groups there is not always an integral number of unit intervals. (Also see Plesiochronous and Isochronous.)

Attenuation—1. The decrease in intensity of an electromagnetic signal as a result of absorption or reflection of energy due to the various characteristics of the path or circuit over which the signal is traveling. Attenuation is usually expressed in decibels. 2. A decrease in intensity of a signal, beam, or wave as a result of absorption of energy and of scattering out of the path of a detector, but not including the reduction due to geometric spreading (i.e., the inverse square of distance effect).

Atto (a)—A prefix used to denote one quintillionth (10-18)

Attributes—The properties of discernible manifestations of the components of a system. These attributes characterize the parameters of a system.

Audio—1. Generally refers to sound frequencies (tones) which can be heard by the human ear (usually between 20 hertz and 20,000 hertz). 2. Relating to recording, production, and reproduction of sound, especially the sound portion of a visual information production (e.g., motion picture videotape, slide tape, etc.).

Audiovisual (AV) Production—An AV production is distinguished from other visual information productions by the combination of motion media (e.g., film, tape, or disk) with sound in a self-contained, complete presentation, developed according to a plan or script for the purpose of conveying information to, or communicating with, an audience.

Automated Data Processing (ADP)—An older term referring to the branch of science and technology concerned with methods and techniques relating to data processing largely performed by automatic means. Now largely replaced by the separate disciplines of Computer Science (for software) and Computer Engineering (for hardware).

Automated Data Processing Equipment (ADPE)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception of data or information by a federal agency, or under contract with a federal agency that requires the use of such equipment, or requires the performance of a service, or the furnishing of a product that is performed or produced making significant use of such equipment. Such term includes computers; ancillary equipment; software, firmware, and similar procedures; services including support services; and related resources. Also see **Automated Information System (AIS)**.

Automated Data Processing System (ADPS)—The total complement of all equipment, including computer hardware, firmware, software, communications equipment, and electronic devices designed to operate as an integrated system to achieve a desired data processing objective.

Automated Identification Technology (AIT)—AIT is a suite of technologies that facilitate the capture of information, such as bar codes, optical memory cards, magnetic strips, integrated circuit cards, radio frequency identification tags, movement tracking devices, and others. AIT can be used in a number of diverse environments and applications. The DoD uses AIT to enhance logistics business practices and provide status and location of its assets.

Automated Information System (AIS)—A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information.

Automated Publications Management Program—A computer system for use by customer account representatives. It tracks and manages requisitions, backorders, and distribution of publications at the unit level.

Automated Tools—Software performing a sequence of operations to assist the user in achieving a goal (e.g., within graphics software, functions that align objects, draw circles, and so forth).

Automatic Calling Unit (ACU)—A dialing device supplied by the communication common carriers that permits a business machine to automatically dial calls over the communications network.

Automatic Digital Network (AUTODIN)—A switched network of the Defense Information System which functions as a single, integrated, worldwide, high-speed, computer-controlled, general-purpose communications network.

Automatic Remote Rekeying—Procedure to re-key distant crypto-equipment electronically without specific actions by the receiving terminal operator.

Automatic Secure Voice Communications (AUTOSEVOCOM)—A worldwide switched network designed to provide DoD users with secure voice communications within the Defense Information System.

Availability—A measure of the degree to which an item of equipment or system is in the operable and committable state at the start of a mission, when the mission is called for at an unknown, random point in time. It is the probability that the system is operating satisfactorily at any point in time when used under stated conditions, where the total time considered includes operating time, active repair time, administrative time, and logistics time.

Back Lobe—A lobe, opposite the main lobe, in an antenna pattern (synonymous with Backward Lobe).

Background Noise—The total system noise in the absence of information transmission; it is independent of the presence or absence of a signal.

Backscatter (Wave)—In radio communications, an electro-magnetic wave produced as a result of scattering of the incident wave, through angles greater than 90o with reference to the original direction of travel.

Backup Software—A complete copy of software or data stored on a diskette, disk, or other electronic media.

Backward Channel—In data communications, a channel with a direction of transmission opposite to that in which user information is being transferred. Used for error control or supervisory channel.

Balanced Line—A transmission line consisting of two conductors in the presence of ground capable of being operated in such a way that when the voltages of the two conductors at all traverse planes are equal in magnitude and opposite in polarity with respect to ground, the currents in the two conductors are equal in magnitude and opposite in direction (synonymous with Balanced Signal Pair).

Balanced—Electrical symmetrical with respect to ground. Also see Balanced Line.

Balun—In radio communications, an electronic device for converting from a balanced to an unbalanced (transmission) line. Commonly used in high frequency (HF) radio systems.

Bandwidth—1. The range of consecutive frequencies comprising a band. 2. The difference, measured in Hz, between the lowest and highest frequencies of a signal or transmission. 3. In data communications it is loosely referred to as the amount of data that can be transferred over a network connection.

Base Communications—Facilities, equipment, and services used to communicate within the confines of a post, camp, station, base, headquarters, or federal building to include local interconnect trunks to the nearest commercial central office providing service to the local serving area. It also includes off-premise activity interconnections that are located within the geographical boundary served by the connecting commercial central office.

Base Level C4 Infrastructure—The common-user portion of the base-level C4 systems environment. It includes transmission, switching, processing, system control, and network management systems, equipment, and facilities which support the base as a whole. Examples include the base telephone switches and cable plant, base communications center, network control center, and metropolitan area network (also known as “base communications infrastructure”).

Baseband—In radio communications, the aggregate band of frequencies carried by a radio communications system between its input (modulator) circuit terminals and its output (demodulator) circuit terminals. The baseband represents the intelligence information transmitted over the radio system. "Baseband" (frequencies) is used as an adjective to distinguish equipment from "radio" (frequencies).

Baseline Configuration—A configuration that consists of an inventory of information resources (i.e., hardware, software or data, or any combination thereof) currently operational within the organization.

Baseline—A specification or product that has been formally reviewed and agreed upon, that serves as a basis for further development, and that can be changed only through formal change control procedures or a type of procedure such as configuration management.

Basic Input/Output System (BIOS)—A program stored in read-only memory and accessed automatically each time the system is turned on. It checks the configuration data and performs self-tests to make sure the system is functional. When the checking is complete, the program loads and turns control over to the operating system.

Basic Software—Comprises those routines and programs designed to extend or facilitate the use of particular automated data processing equipment, the requirement for which takes into account the design characteristics of such equipment. This software is usually provided by the original equipment manufacturer (OEM) and is normally essential to, and a part of, the system configuration by the OEM. Examples of basic software are executive and operating programs; diagnostic programs; compilers; assemblers; utility routines, such as sort/merge and input/output conversion routines; file management programs; and data management programs. Data management programs are commonly linked to, or under the control of, the executive or operating programs.

Basic Telecommunications Services—The Federal Communications Commission’s definition of common carrier transmission services which only result in the movement of information and do not involve the manipulation or restructuring of such information.

BASIC—Acronym for **B**eginner’s **A**ll-purpose **S**ymbolic **I**nstruction **C**ode. A widely adapted programming language that uses English words, punctuation marks, and algebraic notation to facilitate communication between the operator or lay person and the computer. A common programming language used on many minicomputers.

Batch Processing—Processing data or the accomplishment of jobs accumulated in advance in such a manner that each accumulation formed is processed or accomplished in the same computer run.

Batched Communication—The transmission of a large body of network data from one station to another without intervening responses from the receiving unit.

Baud—A unit of signaling speed in data transmission equal to the number of discrete conditions or signal events per second. One baud corresponds to a rate of one unit interval per second where the modulation rate is expressed as the reciprocal of the duration in seconds of the unit interval. For example, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud.

Baudot Code—A code for the transmission of data in which five equal-length bits represent one character. In teletypewriter applications, a stop and start element are added to each character.

Beacon—(satellite) In satellite communications, a discrete radio frequency (RF) transmitted by the satellite for the purpose of tracking (of the satellite) by the earth station antenna system. The beacon RF signal is modulated by an identification frequency (tone).

Beam—In radio communications, the main lobe of the radiation pattern of a directional antenna.

Beamwidth—In radio communications, the angle (in degrees) between the half-power points (3 dB points) of the main lobe of the antenna pattern when referred to the peak power point of the antenna pattern.

Beta Test—Second stage in the testing of computer software before the commercial release. Tests are usually conducted outside the company manufacturing the software.

Bias—1. The amount by which the average of a set of values departs from a reference value. 2. A systematic deviation of a value from a reference value. 3. Electrical, magnetic, mechanical, or other force (field) applied to a device to establish a reference level to operate the device.

Bifurcation—A condition where only two outcomes are possible (e.g., on and off, 0 and 1).

Billboard Antenna—A broadside antenna array with flat reflectors.

Binary Code—A code composed by selection and configuration of an entity that can assume either one of two possible states.

Binary Digit (Bit)—1. In pure binary notation, either of the characters 0 or 1. 2. A unit of information equal to one binary decision or the designation of one of two possible and equally likely states of anything used to store or convey information.

Binary File—A file containing characters that are in machine-readable form.

Binary Modulation—The process of varying a parameter of a carrier as a function of two finite and discrete states.

Binary Number—A number expressed in binary notation.

Bipolar Signal—An electrical signal that may assume either of two polarities, neither of which is zero. A bipolar signal is usually symmetrical with respect to zero amplitude (i.e., the absolute values of the positive and negative signal states are nominally equal).

Bipolar—Pertaining to a system that undertakes both positive and negative values.

Bit—A contraction of the term Binary Digit. The smallest unit of information in a binary system of notation. A bit can be one of only two states, on (usually designated as 1) or off (usually designated as 0). Bits are grouped into bytes (8 bits). Computer memory capacity is stated in the number of bytes that can be stored.

Bit Error Rate (BER)—The number of erroneous bits divided by the total number of bits over some stipulated period of time. The BER is usually expressed as a number and a power of 10 (e.g., 5 in 10-6).

Bit Stuffing—1. A synchronization method used in time division multiplexing to handle received bit streams over which the multiplexer clock has no control. 2. The insertion of noninformation bits into data.

Bit-Mapped Display—Display in which every picture element (pixel) of the screen can be referenced individually.

Biternary Transmission—A method of digital transmission in which two binary pulse trains are combined for transmission over a system in which the available bandwidth is only sufficient for transmission of one of the two pulse trains when in binary form. The biternary signal is generated from two synchronous binary signals, operating at the same bit rate. Each biternary signal element can assume any one of three possible states: +1, 0, or -1.

Bitmap—An image stored as an array of bits.

Blueprint—The STEM-B product that documents the C4 systems' baseline, identifies a target base configuration to support present and future requirements of the base, and provides a time-phased plan for logical transition from the baseline to the target configuration. The formal term for blueprint is Base C4 Systems Blueprint.

Boot Tape—A magnetic tape containing a computer's operating system software.

Branching Menu—A menu that, if selected, brings up another menu.

Bridge—1. In data communications, a device that provides connection between two local area networks using the same logical link control procedure, but may use different medium access control procedures. 2. A balanced electrical network; a bridge may be used for electrical measurements such as resistances or impedances.

Broad Application Markings—Markings of general applicability. Examples are: (a) National star insignia; (b) USAF and U.S. AIR FORCE identification; (c) Aircraft serial numbers and identification numbers. (d) Radio call numbers; (e) American flag markings.

Broadband Communications Bus (BCB)—The BCB is a concept for linking non-cockpit airborne communications through a high capacity LAN-like backbone. Information devices may be voice, video, or data, and are connected to a wide array of communications channels, including UHF SATCOM, HF radio and telephone, both while on the ground and in the air.

Broadband System—A communications system with a multichannel bandwidth of 20 kHz or more (also see Wideband System).

Broadcast—1. In data communications, a method of message routing in which the message is transmitted to all nodes in the network. 2. In radio communications, the simultaneous transmission of a signal or message to a number of stations. This is typically a one-way transmission only and does not involve a response to the originator of the transmission.

Brouter—A combined bridge and router that operates without protocol restrictions, routes data using a protocol it supports, and bridges data it cannot route.

Browser—Any computer software program for reading hypertext. (Browsers are usually associated with the Internet and the World Wide Web.)

Browsing—The act of searching through a communications and information system storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

Bubble Memory—A solid state storage device using microscopic magnetic domains in an aluminum garnet substrate. The domains, or bubbles, are circulated within the substrate and are directed to the output by magnetic fields. This technology has the advantage over random-access memory in that it is non-volatile.

Buffer—1. A routine or storage used to compensate for the difference in rate of flow of data, or time of occurrence of events, when transferring data from one device to another. 2. An isolating circuit used to prevent a driven circuit from influencing the driving circuit. 3. To allocate and schedule the use of buffers.

Built-in Font—A font that is built into the read-only memory of a printer (also known as Resident or Hardware Font).

Burn-In Period—A term used to describe a process during which failures of new equipment items or component parts are likely to occur more frequently. The equipment is operated under power for a period called burn-in to eliminate weak components. Items that successfully survive the burn-in will likely perform satisfactorily for extended periods.

Burst—In data communications, a sequence of signals, noise, or interference counted as a unit in accordance with some specific criterion or measure.

Burst Transmission—1. Transmission that combines a very high data signaling rate with very short transmission times. 2. Operation of a data network in which data transmission is interrupted at intervals.

Bus—1. In communications-electronics, one or more conductors that serve as a common connection for a related group of devices. 2. In a computer, an electronic path for sending data from one part of the computer to another part or to an external device. There are two buses within the Central Processor Unit (CPU): the address bus and the data bus. The address bus connects the CPU and memory. The data bus allows connection with external equipment and is identified primarily by its width, measured in bits (8, 16, 32, etc.). The wider the bus path, the higher the "speed" of the computer.

Byte—A sequence of eight consecutive bits, usually shorter than a word, operated on as a unit.

C—An intermediate programming language, in some respects similar to an assembly language, but with many features that support structured programming.

C Band—In radio communications, the frequency band between 4-8 GHz. **NOTE:** Letter designators of radio frequency bands are imprecise and considered legally obsolete.

Cable Television (CATV) System—Distributes one or more television programs by modulated radio frequency or other signals through a cable distribution system to standard television or radio receivers.

Cache (Memory)—In computing, memory location set aside to store frequently accessed data for improved system performance. This is a high-speed buffer Random Access Memory used between the central processor and main memory. It is used to reduce hard disk access time by storing the commands needed to operate the hard disk.

Call Second—A unit of communications traffic, such that one call-second may be defined as one user making one call of one second duration.

Call Sign—In radio communications, any combination of numbers, letters, or pronounceable words, which identify a communications platform, facility, station, unit, or individual. Used primarily to establish and maintain communications.

Campus Area Network (CAN)—Interconnects local area networks (LAN) within a physical work location (or campus). Each major fixed physical location has a single CAN as a backbone. CANs support higher speeds than LANs for rapid message and file transfer between loosely coupled applications that run on multiple workgroup processors (workgroup servers) at a physical location or which run on LAN servers as described above. Workstations and/or terminals do not connect to the CAN; these devices gain access to the CAN only via their LAN connection.

Capability Maturity Model (CMM)—A framework that describes the elements of an effective software process. It describes an evolutionary improvement path toward a disciplined process.

Capacity—In computing, the total number of bytes that can be stored in memory or a disk; the value may be given as either the unformatted or formatted size.

Capture Effect—In radio communications, the effect associated with the reception of frequency modulated signals in which, if two signals are received on the same frequency, only the stronger of the two will appear in the output of the radio receiver.

Card—A flat piece of hardware consisting of electronic components on a fiberglass or plastic foundation. Add-in cards fit into the extension slots on the system board and control the communications between the computer and peripheral devices.

Carrier Frequency—1. The frequency of a carrier wave. 2. A frequency capable of being modulated or impressed with a second (information carrying) signal. 3. In frequency modulation, the carrier frequency is also referred to as the center frequency.

Carrier Power—In an amplitude modulated radio system, the average power supplied to the antenna transmission line by a radio transmitter during one radio frequency cycle under conditions of no modulation.

Carrier Sense Multiple Access (CSMA)—In data communications, a method of providing multiple access to a shared channel in which all stations employ a listen-before-talk transmission logic.

Carrier—1. An electromagnetic signal frequency suitable for modulation by an intelligence-bearing signal to be transmitted over a communications system. 2. An unmodulated radio frequency emission.

Cascading—Downward flow of information across a range of security levels that is greater than the accreditation range of a component part of a network.

Cassegrain Antenna—In radio communications, a type of dish antenna in which a small reflector is mounted at the focal point. The received signals are first reflected by the antenna to this reflector and then reflected once more into the feedhorn mounted at the center of the dish.

Cellular Radio Telephone System—A computer-controlled full duplex telephone service linking low-power portable, mobile, or porta-mobile radio-telephone transceivers to a local telephone switch. The principal feature is the ability to separate and reuse a limited number of radio frequencies in a large network of relatively small geographic cells. Frequencies for telephones moving between adjacent cells often shift to avoid interference with frequencies of other calls.

Cellular Telephone—A portable telephone in a cellular radio system.

Centi (c)—A prefix denoting one hundredth (10-2).

Central Exchange (CENTREX)—A type of private branch exchange service in which incoming calls can be dialed direct to any extension without an operator’s assistance. Outgoing and intercom calls are dialed direct by the extension users. It is the partitioning of a local exchange carrier switch to provide intrapremise dialing with an abbreviated dialing plan and trunking to external networks.

Central Office of Record (COR)—Office of a Federal department or agency that keeps records of accountable COMSEC material held by activities it oversees.

Central Office Trunks—Trunks from the base telephone system to the local telephone company central office. Trunks connect telephones on base to those in the commercial exchange.

Central Office—In telephone communications, the physical location where common carriers terminate customer lines and houses the equipment that interconnects those lines.

Central Printing and Publications Management Organization (CPPMO)—The organization that manages the agency's printing and reprographics program. The Air Force CPPMO is AFDPO/PP.

Central Processing Unit (CPU)—The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Certification—A comprehensive, fully documented evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process. When this documented level of protection and/or risk is considered to be acceptable by the designated approving authority (DAA) the system accreditation can take place.

Certification and Accreditation—In computing, the formal process implementing risk management. It includes risk analysis, certification, and accreditation.

Certified Technical Solution—A detailed and costed description of a C4 system requirement that can be incorporated into the base infrastructure and is compliant with downward directed architectures and standards.

Channel Bank—Equipment, typically in a telephone central office, that performs multiplexing of lower speed, generally digital, channels into a higher speed composite channel. The channel bank detects and transmits signaling information for each channel, and transmits framing information so that time slots allocated to each channel can be identified by the receiver.

Channel Packing—A technique for maximizing the utilization of voice frequency signals used for data transmission by multiplexing a number of low speed data signals into a single higher speed data stream for transmission on a single voice frequency channel.

Channel—1. In telecommunications, a physical or logical path allowing the transmission of information, the path connecting a data source and a data sink, or receiver. 2. The smallest subdivision of a carrier system by which a single type of communications service is provided (e.g., voice channel, data channel).

Channeling Plan—In telecommunications, the plan by which the frequencies within a frequency band are assigned.

Character—Any number, letter, punctuation mark, or space.

Character Set—A group of letters, numbers, and symbols that have some relationship in common. For example, the American Standard Code for Information Interchange (ASCII) character set contains characters that make up the ASCII coding.

Characteristic Frequency—A frequency that can be easily identified and measured in a given emission. A carrier frequency may, for example, be designated as the characteristic frequency (see also **Reference Frequency**).

Characters Per Second (CHPS)—A measure of transmission rate, usually between a terminal device and a computer.

Check Bit—A binary digit derived from and appended to a data item, for later use in error detection and possibly error correction.

Check Word—In communications security, cipher text generated by a cryptographic logic to detect failures in the cryptography.

Chief Information Officer—(CIO) As mandated by Public Law 104-106, "Subdivision E of the Clinger-Cohen Act of 1996" (formerly the Information Technology Management Reform Act [ITMRA] of 1996), the CIO is an official who is appointed by the head of an executive agency, and is assigned overall responsibility to improve the agency's acquisition and use of information and information technology. In the Air Force, SAF/IQ is appointed as the CIO and HQ USAF/SC as the deputy CIO.

Cipher—A cryptographic algorithm--a mathematical function for encryption and decryption.

Cipher Text—Enciphered information.

Ciphony—The process of scrambling voice transmissions, resulting in encrypted speech.

Circuit—1. A communications link between two or more points. 2. An electronic path between two or more points capable of providing a number of channels. 3. A number of conductors connected together for the purpose of carrying an electrical current. 4. The complete path between two end terminals over which one-way or two-way communications may be provided.

Circuit, 2-Wire—A communication channel for transmission or reception of signals.

Circuit, 4-Wire—A communication channel for simultaneous transmission and reception of signals.

Circuit Switching—A networking technique where the source and destination are connected by an exclusive communications path that is established at the beginning of the transmission and broken at the end.

Classes of Telephone Service—DoD has established criteria for classifying telephone service within military departments. Classify Air Force telephones served by either government-owned or commercial telephone systems as official (Classes A, C, and D) or unofficial (Class B). The class of service code is a two- or more-character alphanumeric code. The first character indicates whether the line is for official or unofficial use. The second character indicates the billing mode. The third character indicates subcategories of service.

Classified Information—Official information that has been determined to require, in the interest of national security, protection against unauthorized disclosure and which has been so designated.

Client—In networking, a software application that allows the user to access a service from a server computer (e.g., a server computer on the Internet).

Client-Server Interface—A program that provides an interface to remote programs (called clients), most commonly across a network, to provide these clients with access to some service such as data bases, printing, etc. In general, the clients act on behalf of a human end-user (perhaps indirectly).

Client/Server Model—An architectural model for distributed computing environments. The model identifies two components: clients and servers. Clients are processes that request services and servers are processes that perform services. The client/server model provides the most consistent path to achieve a distributed computing environment capable of supporting the information technology. The client/server model insulates the client from how and where services are provided.

Clinger-Cohen Act of 1996—Public Law 104-106, Subdivision E of the Clinger-Cohen Act of 1996, February 10, 1996; formerly the Information Technology Management Reform Act (ITMRA) of 1996. The Federal act which repealed the Brooks Act and rescinded the Federal information resources management regulations (FIRMR), and superseded them as the primary Federal guidance on information technology acquisition and management. Among other provisions, it renamed Federal information processing (FIP) resources as information technology (IT); transferred overall responsibility for acquiring and managing Federal IT from the General Services Administration (GSA) to the Office of Management and Budget (OMB); it gave IT procurement authority back to the individual agencies; and called for agencies to establish chief information officers (CIO) and participate in an interagency CIO council.

Clipboard—A temporary storage location in a small computer used to transfer data between documents and between applications. Typically, data is transferred to the clipboard by using an application's copy or cut command; data is transferred from the clipboard by the paste command.

Clock—A reference source of timing information for a machine, system, or equipment.

Clocking—A reference source of timing for a machine or system.

Clone—A term used to describe an imitation of an original. Today, nearly all personal computers (PC) are clones of the first IBM microcomputers, the original PC, and PC/AT systems.

Closed Circuit—1. A term used in radio and television transmissions to indicate that the programs are transmitted directly to specific users and not broadcast for general consumption. 2. A complete electrical circuit.

Closed Security Environment—In communications security, an environment that provides sufficient assurance that applications and equipment are protected against the introduction of malicious logic before or during the operation of a system.

Closed System—A system that does not interact significantly with its environment. The environment only provides a context for the system. Closed systems exhibit the characteristics of equilibrium resulting from external rigidity that maintains the system in spite of influences from the environment.

CMOS—Special memory in a computer that stores information about the computer's configuration.

Co-Channel Interference—Interference resulting from two or more transmissions on the same channel.

Coaxial Cable—An electrical cable consisting of a center conductor surrounded by an insulating material and a concentric outer conductor. Coaxial cable is primarily used for video and wideband radio frequency applications.

Coder/Decoder (CODEC)—A device that converts analog signals to digital form for transmission over a digital network and conversion back to their original analog form.

Cold Boot—Procedures performed to load a computer's operating system software following a power-up. Also, the process of trying to clear a perceived problem from a system by deliberately turning a computer device off and back on.

Color Graphics Array (CGA)—A type of video display unit.

Combat Camera—(COMCAM) Visual information documentation covering air, ground, and sea actions of armed forces in combat and combat support operations and in related peacetime training activities such as exercises, war games, and operations.

Combat Information Transport System (CITS)—Provides a common user fiber optic network for integrated information transport of switched voice, data, video, imagery, and telemetry (to include Integrated Services Digital Network [ISDN], Synchronous Optical Network [SONET], and Asynchronous Transfer Mode [ATM] functionality) to essential core building at each Air Force base.

Combiner—In radio communications, a device employed in wideband radio receiving equipment that compares or combines signals received over different radio paths and selects the (demodulated baseband) signal with the better signal-to-noise ratio.

Command and Control (C2)—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Command and Control Support (C2S) System—The C2S system is the primary means through which the joint force commander (JFC) and subordinate warriors control the flow and processing of information. The C2S system allows the JFC to control the flow and processing of information to support decision-making and influence action during the execution of joint operations.

Command and Control Warfare (C2W)—The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information, to influence, degrade or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such action. Command and control warfare is an application of information operations and is both offensive and defensive.

Command Communications Service Designator (CCSD)—In the Defense Information Systems Network (DISN), an eight digit alpha-numeric code assigned to each communications circuit and which identifies the agency requiring the service, purpose and use, category of service, and unique circuit number.

Command Language—In programming, a source language consisting principally of procedural operations, each capable of invoking a function to be executed.

Command Records Manager (CRM)—Records managers at major commands, field operating agencies, direct reporting units, and unified or specifiedcombatant commands for which the Air Force is the executive agent.

Command, Control, Communications, and Computer (C4) System—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. Also called C4 Systems. (DoD)

Command, Control, Communications, and Computer (C4) Systems Blue—print A base level document that provides the engineering plan for C4 managers to modernize the base-level infrastructure with cost-effective, base-wide C4 capability to support digital transmission of voice, data, video, and telemetry needs. It is produced by the base-level systems' telecommunications engineering manager (STEM-B) and documents the C4 systems baseline, identifies a target base configuration to support present and future requirements of the base, and provides a time-phased plan for the logical transition from the baseline to the target configuration.

Command, Control, Communications, Computers, and Intelligence (C4I)—Interoperability Steering Group (ISG) The C4I ISG consists of O-6 level members from the office of the Secretary of the

Air Force, Air Staff, major air commands (MAJCOM), and field operating agencies (FOA). The C4I ISG promotes the interoperability of C4I systems in the Air Force.

Commercial Communications—The circuits, services, equipment, and facilities furnished by the private sector (regulated and non-regulated entities) or foreign communications entities that satisfy telecommunications requirements.

Commercial-Off-The-Shelf (COTS)—Hardware and software products developed, tested, and sold by commercial companies to the general public.

Commercial Visual Information (VI) Production—A completed VI production, purchased off the shelf, from the stocks of a vendor.

Commercially Procurable Work—Printing and binding work that may be obtained through the Defense Printing Service or the Government Printing Office commercial sources, within the customer's time frame and without compromising security.

Committee on Scientific and Technical Information (COSATI)—A committee composed of Federal agency officials with responsibility for operating scientific and technical information systems.

Common Applications Environment (CAE)—The X/Open term for a computer environment in which applications can be ported across X/Open vendor systems. It includes standards for the operating system, languages, networking protocols, and data management.

Common Business-Oriented Language (COBOL)—A computer programming language designed for business data processing.

Common Carrier (CC)—A private company, subject to government regulation (Federal Communications Commission and state), that furnishes the general public with telecommunications services (e.g., a telephone or satellite communications company).

Common Gateway Interface (CGI)—A set of rules that describe how a Web server communicates with another software program (the "CGI program") on the same machine and how the CGI program talks to the Web server. Any software program can be a CGI program if it handles input and output according to the CGI standard.

Common Operating Environment (COE)—The COE provides an approved set of standards that defines the interfaces, services, protocols, and supporting formats required for application portability profiles. The COE integrates numerous elements (building blocks) that make up the total network or system and is the key element of interoperability. The COE provides a familiar look, touch, sound, and feel of the C4I environment to the warrior, no matter where the warrior is employed. Information presentation and C4I system interfaces are maintained consistently from platform to platform, enabling the warrior to focus attention on the crisis at hand.

Common User Circuit—A circuit designated to furnish a communication service to a number of users.

Common User Network—A system of circuits or channels allocated to furnish communication paths between switching centers to provide communication service on a common basis to all connected stations or subscribers. It is sometimes described as a general-purpose network.

Commonality—A quality that applies to materiel or systems possessing like and interchangeable characteristics enabling each to be used, or operated and maintained, by personnel trained on the others without additional specialized training; having interchangeable repair parts and, or components; and applying to consumable items interchangeably equivalent without adjustment.

Communications—A method or means of conveying information of any kind from one person or place to another.

Communications Cover—Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.

Communications Deception—Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

Communications-Electronics—The specialized field concerned with the use of electronic devices and systems for the acquisition or acceptance, processing, storage, display, analysis, protection, disposition, and transfer of information.

Communications and Information—The consolidated Air Force functional area that includes telecommunications, computers, information management, and audiovisual information. In the Air Force, the term Communications and Information is the equivalent of C4, but is the preferred term. There is no approved acronym for Communications and Information.

Communications and Information Mission Support Plan—The guide for acquiring, using, and disposing of communications and information systems. A key feature of this plan is the way it links those systems to the missions and functions of the Air Force. The plan puts communications and information systems in operational context, and it presents an information system investment strategy that will result in air and space forces that work better and cost less.

Communications and Information Systems Officer (CSO)—The officer responsible for communications and information systems and functions at any Air Force organizational level. At base level, the "base CSO" is the commander of the communications unit responsible for carrying out base systems duties, including management of the basewide C4 infrastructure. At the MAJCOM level, the "MAJCOM CSO" is designated by the MAJCOM commander and is responsible for the overall management of the MAJCOMs communications and information assets. For detailed functions and responsibilities, refer to AFI 33-101, *Communications and Information Management Guidance and Responsibilities*.

Communications Link—The cables, wires, or paths that the electrical, optical, or electromagnetic (radio) wave signals traverse between a transmitting (sending) and receiving station.

Communications Network—1. An organization of stations capable of intercommunications, but not necessarily on the same channel. 2. A set of products, concepts, and services which enables the connection of computer systems for the purpose of transmitting data and other forms (e.g., voice and video) between the systems.

Communications Node—A node that is either internal to the communications network (e.g., routers, bridges, or repeaters) or located between the end device and the communications network to operate as a gateway.

Compact Disk-Read-Only Memory (CD-ROM)—An optical device (disk) capable of containing large amounts of information as minuscule indentations on the surface of the disk that are read by an optical laser device. The indentations represent digital bytes (ones and zeroes). CD-ROM disk standard storage is 683 Megabytes (MB); it is 4-3/4 inches in diameter; and weighs 7 ounces. This standard has been established by the International Standards Organization. In actuality, a maximum of 735 MB of information can be stored on a compact disk.

Compander (—contraction of *Compressor* and *Expander*) In high frequency radio communications, a device used on audio (speech) circuits to improve their quality by reducing the effects of noise present on the circuits.

Compartment—Class of information that has need-to-know access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information.

Compartmented Mode—Automated information system security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts have all the following: (1) valid security clearance for the most restricted information processed in the system; (2) formal access approval and signed non-disclosure agreements for that information to which a user is to have access; (3) valid need to know for information to which a user is to have access.

Compatibility—The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference, defined over some range of functions of interest.

Component—In communications and information systems/equipment, an assembly, or part thereof, which is essential to the operation of some larger assembly. It is an immediate subdivision of the assembly to which it belongs. **NOTE:** Proper usage of the term is dependent on the frame of reference.

Composition—The use of phototypesetting or electronic character generating devices to set type and produce camera copy, negatives, plates, or images for printing and microform production. Composition equipment includes: (1) electronic composition devices and output equipment that produce proportionally spaced characters and spaces, multiple type faces, and variable type sizes; (2) systems that use digital computers to perform line justification, hyphenation, and page makeup; (3) Output systems that use cathode ray tubes to generate copies; (4) devices that emulate composition equipment and that are used primarily to produce copy that is printed or micropublished.

Compromise—In communications security, the known or expected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person.

Compromising Emanations—Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information system equipment.

Computer—An electronic device capable of accepting and processing information and supplying the results. It usually consists of input, output, storage, arithmetic, logic, and control units. Synonym: Automated Information System (AIS).

Computer Abuse—Intentional or reckless misuse, alteration, disruption, or destruction of data processing resources.

Computer-Aided Design (CAD)—Sophisticated computer software that helps a person design any type of object on a video display tube. It may allow views in various dimensions. CAD is used to draft many kinds of designs, including paper forms, interactive data-entry screen forms, process flows, and manufactured items. A CAD system may analyze the drafted item for various properties, test its failure points, simulate its machining or use, or simply produce a graphic image for later display or print-out.

Computer Conferencing—Computer conferencing environments combine the merits of document creation, e-mail, and conferencing by allowing groups and subgroups to participate in conferences via computer workstation. Conferees, or invited guests, can drop in or out of conferences or subconferences at will. The ability to trace the exchanges is provided.

Computer Crime—Fraud, embezzlement, unauthorized access, and other crimes committed with the aid of or directly involving an automated information system.

Computer Cryptography—Use of a crypto-algorithm program stored in software or firmware, by a general-purpose computer to authenticate or encrypt and, or decrypt data for storage or transmission.

Computer Emergency Response Team (CERT)—An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems.

Computer Fraud—Computer-related crimes involving deliberate misrepresentation or alteration of data to get something of value, usually for monetary gain. A computer system must have been involved in the perpetration or cover-up of the act, or series of acts, through improper manipulation of input or output data, applications programs, data files, computer operations, communications, or computer hardware, software, or firmware.

Computer Generated—A form created by a functional area system that is approved by the office of primary responsibility and identified in the prescribing directive.

Computer Graphics Metafile (CGM)—Standard for the description, storage, and communication of graphical information in a device-independent manner.

Computer Matching—A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Computer Network—A computer network consists of computers and the communications components required to allow the exchange of information, files, sharing resources, etc.

Computer Network Attack—(CNA) Operations to disrupt, deny, degrade, or destroy, information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND)—Measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

Computer Network Exploitation (CNE)—Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident with foreign AIS that could be used to the benefit of friendly operations.

Computer Output Microform (COM)—Microform produced directly from digital data.

Computer Program—An identifiable series of instructions or statements, in a form acceptable to a computer, prepared to achieve a certain result.

Computer Program Configuration Item (CPCI)—An aggregate of computer program components, modules, routines, and so forth, which satisfy an end-use function and which is designated by the government for configuration management. CPCIs may vary widely in complexity, size, and type to form a special-purpose diagnostic program to a large command and control system. CPCIs represent a requirement, of a set of requirements allocated from the functional baseline of a program/project.

Computer Resources Support—The facilities, hardware, software, documentation, manpower, and personnel needed to operate and support embedded computer systems.

Computer Security (COMPUSEC)—The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.

Computer Security Incident—Any event in which a computer system is attacked, intruded into, or threatened with attack or intrusion.

Computer Software—A set of instructions, rules, routines, or statements that allow or cause a computer to perform a specific operation or series of operations; or source code listings, object codes, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be created or recreated, compiled or recompiled, and produced or reproduced. The term does not include computer databases.

Computer Virus—Foreign information/data inserted in computers that cause destruction, scrambling, or changing of internal operational data or output data transported to exterior devices (e.g., printers, tape units, local area networks, and so forth), or to other files within the computer's system. Viruses are normally spread from one computer system to another via introduction of the virus into a network via floppy disks processed on an infected system and then exported to other computers, or imported by external files from bulletin board downloads. Viruses are sometimes distributed by disks containing new or updated software.

Concealment—A method to achieve confidentiality in which sensitive information is hidden by embedding it in irrelevant data.

Conditioned Circuit—A circuit that has conditioning equipment to obtain the desired line characteristics for voice or data transmission.

Conditioning Equipment—Corrective networks used to equalize the insertion loss versus frequency characteristics and the envelope delay distortion over a desired frequency range of a circuit or line in order to obtain the desired quality of voice or data signals. Also, at junctions of circuits, equipment used to match transmission levels and impedances and to provide equalization between facilities.

Conference for Data System Languages (CODASYL)—A group created by DoD that includes users and manufacturers, and considers the development of COBOL and hardware-independent software for database management.

Confidentiality—1. An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identity of confidential sources. 2. Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Audits—The verification of the configuration item's conformance to specifications and other contract requirements.

Configuration Item (CI)—An aggregation of hardware, firmware, or computer software or any of its discrete portions, which satisfies an end-use function and is designated by the government for separate configuration management. A CI may vary widely in complexity, size, type, from an aircraft, ship, or electronic system to a test meter or round of ammunition. Any item required for logistics support and designed for separate procurement is a configuration item.

Configuration Management—In computer modeling and simulation, a discipline applying technical and administrative oversight and control to identify and document the functional requirements and capabilities of a model or simulation and its supporting data bases, control changes to those capabilities, and document and report the changes. See also Accreditation, Independent Review, Validation, and Verification.

Configuration—A collection of an item's (C4 system) descriptive and governing characteristics, which can be expressed in functional terms (i.e., what performance the item is expected to achieve), and in physical terms (i.e., what the item should look like and consist of when it is built or assembled).

Connectivity—The ability to provide a virtual or real path between two or more end systems.

Consulting Committee on International Telephone and Telegraph—(CCITT) An international committee operating under the auspices of the International Telecommunication Union. The committee makes recommendations on the relevant characteristics of the respective national telecommunications systems that may form part of the international connections.

Contamination—In communications security, the intermixing of data at different sensitivity and need-to-know levels. The lower-level data is said to be contaminated by the higher-level data; thus, the contaminating (higher level) data may not receive the required level of protection.

Context-Sensitive—Computer action or response directly related to the cursor position or specific point in the software (e.g., a help function that displays information about the specific data entry field in which the cursor was located when help was called).

Cookie—On the Internet, a message from a Web browser to a Web server. The browser stores the message on the user's PC in a text file called *cookie.txt*. The message is sent back to the server each time the browser requests a page from the server. The server can use this information to present the user with customized Web pages. The name "cookie" derives from UNIX objects called magic cookies. These are tokens that are attached to a user or program and change depending on the areas entered by the user or program.

Corrective Maintenance—Also called "Unscheduled Maintenance," it includes all unscheduled maintenance actions performed as a result of a system failure and required to restore the system to a specified condition.

Counterinformation (CI)—Counterinformation seeks to establish a desired degree of control in information functions that permit friendly forces to operate at a given time or place without prohibitive interference by the opposing force.

Covert Channel—A communications channel that allows two operating processes to transfer information in a manner that violates the system's security policy.

Credentials—In communications security, information passed from one entity to another, which is used to establish the sending entity's access rights.

Critical Asset—Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical assets may be DoD assets or other government or private assets (e.g., industrial or infrastructure critical assets), domestic or foreign, whose disruption or loss would render DoD critical assets ineffective or otherwise seriously disrupt DoD operations.

Critical Technical Load—That part of the total technical electrical power required to operate the synchronous communications and automatic switching equipment in a communications facility.

Critical Information—Formerly "Essential Elements of Friendly Information (EEFI)".

Critical Infrastructures—National infrastructures whose incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and distribution, banking and finance, transportation, water supply systems, emergency services, and continuity of government.

Critical Processing—Processing that must continue in a correct and uninterrupted manner to support DoD emergency or war plans, preserve human life or safety, or support the mission of the using organization.

Cross-Polarization—In radio communications, refers to the polarization of the transmit and receive antennas of a radio link or system. The use of two transmitters operating on the same frequency, with one transmitter-receiver pair being vertically polarized, and the other pair horizontally polarized. Cross-polarization is a method to improve performance of the radio link by reducing or counteracting the effects of fading of the radio signals.

Crosslink—In satellite communications, the direct transmission link between two orbitting satellites.

Crosstalk—1. The condition in which a signal transmitted on one circuit or channel of a transmission system is detectable in another circuit or channel. 2. Unwanted transfer of energy from one communications channel to another.

Crypto-Ignition Key (CIK)—A key storage device (KSD) that contains information used to electronically lock and unlock a terminal's secure mode.

Current Master File (CMF)—As distinguished from the "Prior Master File," the current state of a data file in an automated system at a given time; or master continuous update tapes (or other media) containing data merged with valid transaction data to create a new (or updated) master file.

Cursor—Visual mechanism to mark, on-screen, where current input or output is to happen.

Custodian—A person who receives publications to post, file, and keep in the publication library.

Customer—Anyone who has an account with an office using publishing distribution offices. This covers customers of all levels from subaccount representative through publishing distribution center.

Cyberspace—The Internet and the connected on-line services.

Data—1. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned. 2. A general term used to denote any or all facts, numbers, letters, and symbols that refer or describe an object, idea, condition, situation, or other factor.

Data Administrator—A person or group that ensures the utility of data used within an organization by defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical database designs, and defining data security procedures.

Data Architecture—A framework for organizing data into a manageable grouping to facilitate shared use and control throughout the Air Force.

Data Attribute—A characteristic of a unit of data such as length, value, or method of representation.

Data Bank—A comprehensive collection of data which may be structured as follows: one line of an invoice may form an item; a complete invoice may form a record; a complete set of such records may form a file; and the collection of files used by an organization may be known as its data bank.

Data Base—1. Information that is normally structured and indexed for user access and review. Data bases may exist in the form of physical files (folders, documents, and so forth) or formatted automated data processing system data files. 2. A structured or organized collection of information, which may be accessed and manipulated by the computer. 3. A set of data that is required for a specific purpose that is fundamental to a system, project, enterprise, or business. A data base may consist of one or more data banks and be geographically distributed among several repositories. Data bases may exist in the form of physical files or formatted automated data processing system data files.

Database Administration—1. The analysis, classification, and maintenance of an organization's data and data relationships. It includes the development of data models and dictionaries, which combined with transaction processing, are the raw materials for data base design. It includes the development of data models and dictionaries, which combined with transaction processing, are the raw materials for data base design. 2. The activity responsible for enforcing policies and standards set by the data base administrator, to include providing technical support for physical data base definition, design, implementation, maintenance, integrity, and security, and coordinating with computer operations technicians, system developers, vendors, and users.

Data Base Management System (DBMS)—A software system used to access, retrieve, and otherwise manage the data in a data base.

Data Circuit-Terminating Equipment (DCE)—The interfacing equipment sometimes required to couple the data terminal equipment into a transmission circuit or channel and from a transmission circuit or channel into the data terminal equipment.

Data Code—A number, letter, character, or any combination thereof used to represent a data element or data item. For example, the data codes E8, 03, and 06 might be used to represent the data items of sergeant, captain, and colonel under the data element military personnel grade.

Data Communications Protocol Standards (DCPS)—A standardization area of the Defense Standardization Program. This area establishes DoD protocol standards and reference protocol architectures necessary to support Intranet work host-to-host data communications using digital communications techniques. The DCPS area involves standardization of Internet work, peer, and interlayer management protocols, including those that deal with end-to-end (host-to-host) communications across a network or a concatenated set of networks.

Data Compression—The process of reducing bandwidth, cost, and time for the generation, transmission, storage of data by employing techniques designed to remove data redundancy. Data compression standards specify algorithms for compressing data for exchange over a network; it can reduce communications loading by as much as 80 percent without affecting the form of transmitted data.

Data Concentrator—A functional unit that permits a common transmission medium to serve more data sources than there are channels available within the transmission medium.

Data Dictionary—A specialized type of data base containing metadata, and managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and data bases; an application of a data dictionary system.

Data Dictionary/Directory Services—Key computer software tools that manage data and information resources. Such services provide extensive facilities for recording, storing, and processing descriptions of an organization's significant data and data processing resources, and often provide facilities to use metadata (information about data).

Data Element—A basic unit of information built on standard structures having a unique meaning and distinct units or values. Examples of data elements are: rank, grade, age, etc.

Data Field—The defined area, usually a column or columns, on a numbered line or block, where you enter a data element.

Data File—Related numeric, text, or graphic information that is organized in a strictly prescribed form and format.

Data Fusion—In command and control (C2) operations, the bringing together of fusing of independently obtained data to obtain a bigger picture of the whole (e.g., data obtained from sensors that are significantly different, such as a video image being fused with information from a radio transmission.)

Data Integrity—1. A property of data in which all assertions (accurate, current, consistent, complete) hold. 2. The assurance that the data received is the same data as the data that was sent. 3. The concept that the data base management system will perform its function consistently, preserve data without unintentional change, produce correct results to the defined degree of precision, and maintain data availability.

Data Interchange Standards Association (DISA)—A non-profit organization that administers the X.12 standard for the ANSI X.12 subcommittee and provides news updates on electronic data interchange.

Data Item—A subunit of descriptive information or value classified under a data element. For example, the data element "military personnel grade" contains data items such as sergeant, captain, and colonel.

Data Management—The function of controlling the acquisition, analysis, storage, retrieval, and distribution of data.

Data Processing—1. Any procedure for receiving information and producing a specific result. 2. Executing sequences of operations on data, such as merging, sorting, calculating, and printing.

Data Repository—A repository provides a place and method to store metadata. It generally is broader and supports more kinds of data than a data dictionary.

Data Resource—Any data created manually or by automatic means and used by a system or enterprise to represent its information.

Data Server—The data server provides data services to clients. A client will send a request to a data server (sometimes called a "database server") and the server will respond with the results of the request. The accessing and updating of the data maintained on the data server is performed by the data server, not by the clients. It supports the implementation of better controls by managing access to the data resident within the server. The data server can also be optimized to the type of data it is being asked to manage; a data server could support archiving and be based on optical storage technology rather than magnetic.

Data Sink—A device that receives data signals from a data source.

Data Steward—A person or group that manages the development, approval, and use of data within a specified functional area, ensuring that it can be used to satisfy data requirements throughout the organization.

Data Storage and Archiving—Data storage and archiving services provide a database application with the facilities for temporary storage and long-term archiving of data. Archiving files is a process where the information contained in an active computer file is made ready for storing in a nonactive file, perhaps in off-line or near-line storage. Typically, when files are archived, they are compressed to reduce their size. To restore the file to its original size requires a process known as "unarchiving".

Data Structure—The framework that defines the specifics about one or more types of data that support the user system. The data structure includes the collection of record types, linkages, fields, entry points, and integrity rules.

Data Systems Authorization Directory (DSAD)—The official HQ USAF-approved directory of data system descriptions with assigned data system designators and authorized for processing by Air Force activities. It is an inventory of authorized data systems and reflects Air Force activities authorized to process individual applications and the specific types of automated data processing equipment on which the applications are processed. System descriptions contained in the DSAD may be for systems under development or in operation. The status of an individual system can be determined by the implementation schedule or the activities responsible for the design, implementation, and maintenance. The DSAD is published by the Standard Systems Group.

Data Terminal Equipment (DTE)—Equipment consisting of digital-end instruments that convert the user information into data signals for transmission or reconvert the received data signals into user information. The functional unit of a data station that serves as a data source of a data link and provides for the data communication control function to be performed in accordance with link protocol. The DTE may consist of a single piece of equipment that provides all the required functions necessary to permit the user to intercommunicate, or it may be an interconnected subsystem of multiple pieces of equipment, to perform all the required functions.

Data Transfer Rate—A particular rate at which data is transmitted through a channel but measured during the time the data is actually being transmitted.

Debug—In computing, the process to locate and correct errors in a computer program.

Decals or Film Marking—Designs, words, or numerals on specially prepared adhesive film or paper that is affixed to aircraft, buildings, vehicles, and other objects.

Decibel (dB)—In communications-electronics, the standard unit for expressing transmission or signal gain or loss and relative power ratios. The decibel is one-tenth of a bel, which is too large a unit for convenient use. Both units are expressed in terms of the logarithm to the base 10 of the ratio of two levels of power.

Decryption—e restoration of encrypted data to its original plain text or other readily usable state.

Dedicated Server—computer (or node) on which applications are limited to maintaining network resources. No user applications are available.

Dedicated Systems—formation processing components devoted to satisfying a unique mission or functional information need beyond the capability of shared systems; functional end-user organizations generally control these resources.

Defense Automated Visual Information System (DAVIS)—standard DoD-wide automated data processing system for visual information (VI) management purposes at DoD component and major command levels. It includes a production data base covering production, acquisition, inventory, distribution, product status, and archival control of audiovisual productions and VI materials, and VI facilities' data base that includes activities, facilities, personnel, and funds.

Defense Commercial Telecommunications Network (DCTN)—leased communications system that provides common user switched voice, dedicated voice and data, and video teleconferencing services throughout the United States. This fully integrated digital network uses satellite and terrestrial transmission to serve U.S. Government installations nationwide. The DCTN interfaces with the Defense Switched Network and the Federal Telephone System 2000.

Defense Data Network (DDN)—Component of the Defense Communications System that handles DoD voice, data, and video communications. DDN is the DoD worldwide digital data communications backbone for Warner-exempt systems. The DDN provides a common-user, packet-switched data communications network for DoD agencies. The DDN provides worldwide, survivable data subnetworks for UNCLASSIFIED through TOP SECRET and SENSITIVE-COMPARTMENTED INFORMATION. DDN is owned, operated, and controlled by the Defense Information System Agency. See also Defense Switched Network.

Defense Information Infrastructure (DII)—The DII is the web of communications networks, computers, software, data bases, applications, and other services that meet the information processing and transport needs of DoD users, across the range of military operations. The DII includes the information infrastructure of the Office of the Secretary of Defense, the military departments, the Chairman of the Joint Chiefs of Staff, the Defense agencies, and the combatant commands. It provides information processing and services to subscribers over the Defense Information System Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information. The DII is embedded within and deeply integrated into the National Information Infrastructure. Their seamless relationship makes distinguishing between them difficult.

Defense Information Infrastructure Common Operating Environment—(DII COE) The DII COE concept is a fundamentally new approach which emphasizes both software reuse and interoperability; however, it is much broader in scope than simple software reuse. The DII COE is not a system; it provides a foundation for building open systems. It is a "plug-and-play" open architecture designed around a client/server model; it offers a collection of services and already built modules for mission application. The DII COE is also an evolutionary acquisition and implementation strategy. It emphasizes incremental development and fielding to reduce the time required to put a new functionality into the hands of the user.

Defense Information System (DIS)—The DIS is a composite of DoD owned and leased telecommunications subsystems and networks comprised of facilities, personnel, and material under the management control and operational direction of the Defense Information Systems Agency. It provides the long haul, point-to-point, and switched network telecommunications needed to satisfy the requirements of DoD and certain other U.S. Government agencies.

Defense Information Systems Agency (DISA)—A U.S. Government agency with the mission to exercise operational direction and management control of the Defense Information System to meet the long haul, point-to-point, and switched network telecommunications requirements of the National Command Authorities, DoD, and other U.S. Government agencies as authorized and directed by the Secretary of Defense.

Defense Information Systems Agency Information Network (DISANET)—DISANET is DISA's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting DISA's operations. It is transparent to its users, facilitates the management of information resources, and is responsive to DISA's missions and needs. DISANET is a sub-element of the DISA Information System.

Defense Information Systems Network (DISN)—The DISN is an enhanced long-haul telecommunications infrastructure that supports a full range of communications services (voice, data, and video) for DoD activities worldwide. It is a dynamic network, with the capability to accommodate emerging new or improved technologies. The DISN provides the primary transmission path to support the Defense Information Infrastructure.

Defense Information Operations (DIO)—The DIO process integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and to defend information systems. DIOs are conducted through information assurance, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special information operations.

Defense Message System (DMS)—DMS is a flexible, secure, commercial-off-the-shelf (COTS) based system providing multi-media messaging and directory services taking advantage of the underlying Defense Information Infrastructure network and services. DMS is a new way of doing electronic organizational messaging. DMS is eliminating the need for the Automatic DMS is a integrated suite of applications designed to run on the Defense Information System Network (DISN). DMS is NOT a network and is the system of record for "ORGANIZATIONAL" messaging and services.

Defense Printing Service (DPS)—The service that manages the DoD consolidated printing and duplicating organizations. The DPS is a subordinate unit of the United States Navy, who is the executive agent for DoD printing.

Defense Red Switch Network (DRSN)—A network of the Defense Information System Network consisting of a global secure voice switching network whose subscribers are served by a variety of automatic switches and manual operator switchboards. All switchboards are interconnected within the network by dedicated wideband trunk circuits and/or narrowband Defense Switched Network.

Defense Satellite Communications System (DSCS)—The worldwide military satellite network managed by the Defense Information Systems Agency, comprising orbiting space segments and ground terminals and control segments that operate in the super-high frequency band to provide long-haul multi-channel communications connectivity.

Defense Switched Network (DSN)—The DSN is the switched circuit telecommunications system of the DISN. It provides end-to-end common-user and dedicated telephone service, voice-band data, and video teleconferencing for the DoD. The DSN provides rapid and low-cost long haul, secure and non-secure voice, data, and video services throughout the DoD.

Defensive Counterinformation (DCI)—Activities which are conducted to protect and defend friendly information and information systems.

Defensive Information Operations (DIO)—The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. DIOs are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. DIOs ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.

Degaussing—The neutralization or removal of the magnetization of a mass of magnetic material. Degaussing renders any stored data on magnetic media unreadable and is used in the sanitizing of magnetic storage tapes, and computer disks and diskettes. Also called demagnetizing.

Delay Equalizer—An electronic corrective network designed to make the phase or envelope delay of a circuit or system substantially constant over a desired frequency range.

Delay Line—A real or artificial transmission line or equivalent device designed to introduce specific time delays to the signals passing through the line.

Delta Modulation—A technique for converting an analog signal to a digital signal.

Demand Assignment—In satellite communications, an operational technique where various users share a satellite capacity on a real-time demand basis. A user needing to communicate with another user of the network activates the required circuit; upon completion of the communication, the circuit is deactivated and the satellite capacity is made available for other users.

Demodulation—The reverse of modulation. A technique where the modulated signal is processed (demodulated) to retrieve the original modulating (input) signal.

Demultiplex—The reverse of multiplex. Compare modulation and demodulation.

Denial Authority—The individuals with authority to deny requests for access or amendment of records under the Privacy Act and the Freedom of Information Act.

Density—The closeness of space distribution on a storage medium.

Department of Defense Directive (DODD)—A broad DoD policy document containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by DoD components within their specified areas of responsibilities. DODDs establish or describe policies, programs; and organizations; define missions; establish organizations; provide authority; and assign responsibilities. One-time tasking and assignments of deadlines are not appropriate in DODDs.

Department of Defense Directive-Type Memorandum—A memorandum issued by the Secretary of Defense, Deputy Secretary of Defense, or Office of the Secretary of Defense Principal Staff Assistants (PSA) that, because of time constraints, cannot be published in the DoD Directives System. Directive-type memorandums signed by PSAs are procedural in nature. They implement policy documents, such as DoD directives, Federal laws, and Executive Orders. Directive-type memorandums signed by the Secretary or Deputy Secretary of Defense are policy-making documents. A directive-type memorandum shall be converted into a DoD directive or DoD instruction within 90 days, unless the subject is classified with limited distribution or is material of limited or temporary relevance.

Department of Defense Directives System Transmittals—The notice that changes or cancels a DoD directive, DoD instruction, or DoD publications.

DoD Instruction (DODI)—A DoD issuance that implements the policy, or prescribes the manner or a specific plan or action for carrying out the policy, operating a program or activity, and assigning responsibilities.

Department of Defense Intelligence Information System (DODIIS)—1. The aggregation of DoD personnel, procedures, equipment, computer programs, and supporting communications that supports the timely and comprehensive preparation and presentation of intelligence and intelligence information to military commanders and national-level decision-makers. 2. DODIIS represents a worldwide computer network linking intelligence data-handling systems. These information systems support the collection, production, and dissemination of various defense intelligence products. DODIIS consists of approximately 40 nodes and is characterized by various means of intelligence input processing.

Department of Defense Issuances—DoD directives, instructions, publications, and their changes.

Department of Defense Publications—DoD issuances that implement or supplement DoD directives and instructions by providing uniform procedures for management or operational systems and disseminating administrative information. DoD publications include catalogs, directories, guides, handbooks, indexes, inventories, lists, manuals, pamphlets, plans, regulations, and standards that implement or supplement DoD directives or DoD instructions.

Department of Defense Standardized Profile—An internationally agreed to, harmonized document that identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.

Departmental Printing—Printing (such as publications, forms, and visual aids) used throughout the Air Force, regardless of origin. AFPDO/PP buys departmental printing through the Defense Printing Service and the Government Printing Office.

Desktop Publishing—Software programs using a microcomputer (and usually a component of an office automation system) to electronically arrange text and graphics as composition. Output is then produced on an electronic laser printer, ink jet printer, or similar output device in a page format. The output may be reproduced using printing methods.

Dial Central Office (DCO)—A private telephone exchange/switch that usually includes access to the public switched network, which provides dial service on subscribers' premises and serves only their stations with local and trunked communications.

Dibit—A group of two bits. The four possible states for a dibit are 00, 01, 10, and 11.

Dichroic Filter—An optical filter that reflects one or more optical bands or wavelengths and transmits others, while maintaining a nearly zero coefficient of absorption for all wavelengths of interest. A dichroic filter may be high-pass, low-pass, band-pass, or band rejection.

Differential Modulation—A type of modulation in which the choice of the significant condition for any signal element is dependent on the choice for the previous signal element. Delta Modulation is an example.

Differential Phase Shift Keying (DPSK)—A method of modulation employed for digital transmission. In DPSK each signal element is a change in the phase of the carrier with respect to its previous phase angle.

Diffraction—The bending of light, radio, or sound waves around an object, barrier, or aperture.

Digital Distribution Unit (DDU)—A device designed to take a digital input and transmit the signal in a quasi-analog form over a voice grade telephone line and vice versa. The most popular version uses a differential diphase modulation scheme that combines timing and data into one composite signal.

Digital Multiplexer—An electronic device for combining several digital signals into an aggregate bit stream.

Digital Patch and Access System (DPAS)—A semi-automated patch and access system to provide the Defense Information System with the means to rapidly reconfigure digital circuits. The cross-connect capability of a DPAS permits the assignment and redistribution of channels on T1 carriers (DS-1 rate 1.544 Mbps) which use digital transmission systems.

Digital Signal (DS)—In telecommunications (1) a nominally discontinuous electrical signal that changes from one state to another in discrete steps. The electrical signal could change its amplitude or polarity (analog signals may be converted to digital signals by a process called quantizing); (2) a signal in which discrete steps are used to represent information. **NOTE:** In the North American digital hierarchy, designators for the DS level hierarchy correspond to the designators for T-carrier. (a) Digital Signal 0 (DS0): A basic digital signal rate of 64 kbps, corresponding to the capacity of one voice-frequency equivalent communications channel. (b) Digital Signal 1 (DS1): A digital signal rate of 1.544 Mbps, corresponding to the North American T-1 designator. © Digital Signal 2 (DS2): A digital signal rate of 6.312 Mbps, corresponding to the North American T-2 designator. (d) Digital Signal 3 (DS3): A digital signal rate of 44.736 Mbps, corresponding to the North American T3 designator. (e) Digital Signal 4 (DS4): A digital signal rate of 274.176 Mbps, corresponding to the North American T-4 designator. (f) Digital Signal 5 (DS5): A digital signal rate of 400.352 Mbps, corresponding to the North American T-5 designator.

Digital Signature—1. A non-forgeable transformation of data that allows proof of source, non-repudiation, and verification of data integrity. 2. A method of ensuring that a message was sent by the person claiming to send it. The signature is encrypted with the sender's private key and decrypted by the recipient using the sender's public key. Since only the sender could have encrypted the signature, the recipient is assured of the sender's identity.

Digital Signature Standard (DSS)—A cryptographic technique for authenticating electronic communications conforming to IEC 9796 International Digital Signature Standard and developed by the National Security Agency as part of the U.S. Government's CAPSTONE program.

Digital Subscriber Terminal Equipment (DSTE)—Basic input/output devices that include paper tape, punch cards, teletypes, and teletypewriters in a telecommunications center. This equipment is over 20 years old and is being replaced with standard remote terminals.

Digital Video Disk (DVD)—A storage format that can pack 4.5 GB of data on a disk that resembles a compact disk.

Digitize—To convert an analog signal to a digital signal.

Digroup—Abbreviation for "digital group." A term designating the basic digital multiplexing grouping. In the United States, this basic group is derived from 1.544 Mbps; in Europe, the basic group is commonly 2.048 Mbps.

Diplex Operation—Simultaneous one-way transmission or reception of two independent signals using a common element, such as an antenna system or a channel.

Diplexer—In radio communications, a multi-port coupling device which permits two transmitters or receivers to operate simultaneously without interaction using the same antenna system.

Direct Broadcast Satellite (DBS)—A new, high-powered, national satellite distribution system for video, audio, and data. The system consists of approximately 150 channels of standard resolution television that offers both standard 4:3 and wide screen 16:9 aspect ratios. DBS has potential for the Air Force and DoD to broadcast high volumes of information at speeds in the multi-megabit range to a wide variety of users throughout a theater of operations.

Direct Current (DC) Erasure—Degaussing with a hand-held permanent magnet or with DC electrical-powered equipment to saturate the media so the noise level is raised to mask the signal level. There should be no signal level detectable above the noise level after DC erasure.

Direct Data Exchange (DDE)—In data communications, the exchange of data between programs. Any changes made to the data in the source (server) application will automatically and dynamically be changed also in the current (client or receiving) application. The data in the current (client or receiving) program is said to be linked to that program.

Direct Memory Access (DMA)—In memory systems, a technique that allows a peripheral device to gain direct access to the main memory of the computer. When the peripheral initiates DMA the processor is compelled to stop all bus activity while the peripheral occupies the bus.

Directed Energy—An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles.

Director of Information Management (IM)—As used here, IM may refer to a Chief, Base Information Management. Depending on the organizational level, this official may supervise a publishing distribution office and a master publication library within the 16G1-series of functional account codes (formerly FAC 11XX) at installation level.

Directory—1. In programming, a record containing details of the location of a file held in backing storage that is accessed by the operating system. 2. In data bases, a file that stores relationships between records in other files. 3. In data communications, a table containing routine information.

Directory Information Tree (DIT)—A directory information base organizational model that uses a hierarchical tree structure.

Disclosure—Giving information from a system, by any means, to anyone other than the record subject.

Discriminator—That part (stage) of a frequency modulation (FM) radio receiver that extracts the desired intelligence signal from an incoming FM carrier wave by changing frequency variations of the signal into amplitude variations (baseband or audio signals). Opposite of a Modulator in a FM radio transmitter.

Disk (or Disc)—A circular, flat magnetic-sensitive rotating device that contains data.

Disk Drive—In memory systems, a mechanism for rotating a disk pack or a magnetic disk and controlling its movements.

Disk Operating System (DOS)—1. An operating system for computers with disk drives in which relevant routines are loaded from disk as required. 2. A program that controls the way programs are loaded into memory, how information is stored on the disk, and how the computer communicates with the printer and other peripheral devices.

Diskette—A thin flexible plastic disk encased in a protective envelope that is inserted into a disk drive to magnetically store and read data (see Disk).

Diskless Workstation—A workstation that does not have a fixed (hard) or removable (floppy) disk drive. It is essentially a smart terminal that handles only presentation management. All processing and storage of interim data reside on the server. Diskless workstations can provide a better measure of cost efficiency and security than other end-user processing platforms.

Display Equipment—Any device that displays miniaturized information or documents, such as cathode ray tube displays or microform viewers.

Disposition—1. A comprehensive term that includes destruction, salvage, or donation; transfer to a staging area or records center; transfer from one organization to another. 2. Actions taken with inactive records. These actions may include erasure of data, transfer to a records center, or transfer to the National Archives.

Disposition Instructions—Precise instructions, specifying the date or event for cutoff, transfer, retirement, or destruction of records.

Distributed Data Base—1. A data base that is not stored in a central location but is dispersed over a network of interconnected computers. 2. A data base under the overall control of a central database management system but whose storage devices are not all attached to the same processor. 3. A data base that is physically located in two or more distinct locations.

Diversity Reception—That method of radio frequency (RF) reception where, in order to minimize the effects of fading, a resultant signal is obtained by combination or selection, or both, of two or more independent RF signals that carry the same modulation or intelligence. Used primarily in microwave radio systems. Examples of diversity are frequency, space, and polarization diversity.

Document—Recorded information in paper or some other medium.

Document Reader—A device capable of reading documents into a computer.

Documentation—1. The act or process of substantiating by recording actions and/or decisions. 2. Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, codebooks, record layouts, user guides, and output specifications.

Domain—1. The independent variable used to express a function. Examples of domain are time, frequency, and space. 2. In distributed networks, all the hardware and software under the control of a specific set of one or more host processors.

Domain Naming System (DNS)—A static, hierarchical data base used with Transfer Control Protocol/ Internet Protocol hosts, and is housed on a number of servers on the Internet; it allows users to specify remote computers by host names rather than numerical Internet Protocol addresses.

Dot Matrix—1. In computer graphics, a two-dimensional pattern of dots used for constructing a display image. This type of matrix is used to represent characters by dots. 2. In printing, a pattern of dots used as the basis for character formation in a matrix printer.

Dot Pitch—In peripherals, the distance between two corresponding dots in two adjacent triads.

Double Density—In memory systems, a technique to increase the storage capacity of a floppy disk. The packing density is increased by modified frequency modulation recording techniques.

Double Sideband—In radio communications, the frequency bands occupied by a modulated carrier wave, above and below the carrier frequency.

Double Sided—In memory systems, pertaining to a technique to increase the total storage capacity of a floppy disk by recording data on both sides of the disk.

Down-Converter—In radio communications, a device, generally in the receiving equipment, which translates or converts the input signal frequencies in such a manner that the output frequencies are lower in the spectrum than the input frequencies. The frequency translation process does not alter the intelligence contained in the input signal.

Downlink—In satellite communications, that portion of a satellite link involving transmission of a signal from the satellite to the earth terminal. It is the opposite of uplink.

Drivability—In data communications, drivability refers to the ease with which users may transfer from one application to another with minimal interference, errors, confusion, relearning, or retraining. Drivability relates only to those aspects for which consistency is necessary to promote easy transfer among conforming environments.

Dual Diversity—The simultaneous combining of (or selection from) two independently fading signals, so that the resultant signal can be detected through the use of space, frequency, angle, time, or polarization characteristics.

Dumb Terminal—In peripherals, a terminal (or computer using dumb terminal software) that allows communications with other computers, but does not enhance the data exchanged or provide additional features.

Duplex Cable—A fiber optic cable composed of two fibers.

Duplex Circuit—A circuit that permits transmission in both directions. For simultaneous two-way transmission, see Full-Duplex Circuit.

Duplexer—In radio communications, a three-port frequency dependent device that may be used as a separator or a combiner of signals. It allows simultaneous transmission and reception of two signals of different frequencies using a single antenna system with isolation between the two signals.

Duplicating—Producing material in one color, using an electrostatic process; stencil, master, or offset plate not made with an intermediate film.

Duplicating Center—A reproduction facility capable of producing duplicating work only. The host command manages and operates it to serve all customers on the installation. (1) Duplicating Branch. A satellite of a duplicating center staffed and managed by the center. It is set up at a specific location to do work that cannot be done at the center. (2) Duplicating Facility. An activity that is managed by the host but staffed by an activity other than the duplicating center.

Duplicator—A one- or two-unit (including tandem or perfecting) sheet-fed offset press or an automatic electrostatic or thermal copy-processing machine. The maximum image size is 273 by 362 millimeters (10-3/4 by 14-1/4 inches), and the maximum paper size is 279 by 432 millimeters (11 by 17 inches). Speed of the duplicator exceeds 70 copies per minute.

Durability—The probability that an item of equipment or system will perform its intended function for a specified interval under stated conditions without major failures.

Dynamic Random Access Memory (DRAM)—In a computer, a random access data storage method in which the memory cells require periodic electrical refreshing to avoid loss of data held. DRAM is erasable and reprogrammable. DRAM will lose its contents when the power is removed (volatile memory).

Earth Coverage—In satellite communications, the condition obtained when a beam from the satellite is sufficiently wide to cover the surface of the earth exposed to the satellite. Also see **Footprint**.

Earth Segment—The earth segment includes all equipment not in space orbit and capable of communicating with a satellite. Such equipment may be airborne, shipborne, or land-based. The earth segment may be divided into three basic functions: (1) Those using the satellite for operational communications; (2) Those for satellite communications control; and, (3) Those that exercise satellite control. These three functions may use the same terminal, the same type of terminal, or other terminal variations including completely separate facilities.

Earth Station—A station located either on the Earth's surface or within the major portion of the Earth's atmosphere and intended for communication with one or more space stations, or with one or more stations of the same kind by using one or more reflecting satellites or other objects in space.

Edit—To change, add, delete, or move individual blocks of data in a data base.

Effective Radiated Power (ERP)—In a radio transmission system, the power supplied to the antenna multiplied by the power gain of the antenna in a given direction.

Electrically Alterable Read-Only Memory (EAROM)—A read-only memory that can be modified electrically while connected in-circuit. Synonymous with Electrically Erasable Read-Only Memory.

Electrically Erasable Programmable Read-Only Memory (EEPROM)—A special kind of ROM that can be electrically erased and reprogrammed. It can be erased by an electrical signal rather than by exposure to ultraviolet light.

Erasable Programmable Read-Only Memory—(EPROM) ROM that is erasable and reprogrammable. This type of ROM is usually erased off-circuit, usually by exposure to an ultraviolet light source.

Electromagnetic Compatibility (EMC)—The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

Electromagnetic Deception—The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability.

Electromagnetic Expendables—Nonrecoverable electronic warfare devices, such as chaff, flares, unmanned vehicles, decoys, and unattended jammers.

Electromagnetic Interference (EMI)—Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance or electronic/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like.

Electromagnetic Intrusion—The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion.

Electromagnetic Jamming—The deliberate radiation, re-radiation, or reflection of electromagnetic energy to prevent or reduce the enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

Electromagnetic Radiation (EMR) Hazards—Hazards caused by a transmitter/antenna installation that generates electromagnetic radiation in the vicinity of ordnance, personnel, or fueling operations in excess of established safe levels or increases the existing levels to a hazardous level; or a personnel, fueling, or ordnance installation located in an area that is illuminated by electromagnetic radiation at a level that is hazardous to the planned operations or occupancy. These hazards will exist when an electromagnetic field of sufficient intensity is generated to: (1) induce or otherwise couple currents and/or voltages of magnitudes large enough to initiate electro-explosive devices or other sensitive explosive components of weapon systems, ordnance, or explosive devices; (2) cause harmful or injurious effects to humans and wildlife; and, (3) create sparks having sufficient magnitude to ignite flammable mixtures of materials that must be handled in the affected area. Also called EMR Hazards, RADHAZ, HERO.

Electromagnetic Spectrum—The total range of frequencies over which any form of electromagnetic radiation occurs. The lowest frequencies are radio waves; increases in frequency-produce infrared, visible light, ultraviolet, x-rays, gamma radiation, and cosmic rays. The electromagnetic spectrum was, by custom and practice, formerly divided into 26 alphabetically designated bands. This usage still prevails to some degree; however, the International Communications Union formally recognizes 12 bands from 30 hertz to 3000 gigahertz.

Electronic Bulletin Board (EBB)—1. A system that connects users and a common computer host. Used to exchange software programs, technical information, and other information and data. 2. A computer with software that permits individuals to dial up via modem and exchange electronic mail messages with other users of the system. Bulletin boards are frequently composed of news groups that share information on a wide range of topics, from recreational activities, to political and social issues, to the latest advances in computer and engineering technology. These systems are often used for exchange of computer programs and other files that are of interest to other users of the bulletin board community. Users are permitted to download files and programs (uncopyrighted software, commonly known as **Shareware**) from the bulletin board in exchange for sharing their software innovations with others on the system.

Electronic Commerce (EC)—The conducting of business communications and transactions over networks and through computers. As most restrictively defined, EC is the buying and selling of goods and services, and the transfer of funds, through digital communications. But, EC also includes all intercompany and intracompany functions (such as marketing, finance, manufacturing, selling, and negotiation) that enable commerce and use electronic mail, electronic data interchange, file transfer, facsimile, video conferencing, workflow, or interaction with a remote computer (including use of the World Wide Web).

Electronic Data Interchange (EDI)—The computer-to-computer exchange of business documents in a standard format by a computer-based communications system. This business procedure replaces paper versions of a variety of business documents such as purchase orders, shipping notices, invoices, receipts, inventories, payments, etc.

Electronic Data Interchange for Administration, Commerce, and Trans—port (EDIFACT) A United Nations-sponsored global set of EDI standards. EDIFACT is derived from the X.12 standards but incorporates additional and different segments and uses a more flexible and generic approach to defining data elements using qualifier code.

Electronic Data Processing—Data processing performed largely by electronic equipment.

Electronic Form—A form created, manipulated, and outputted from a computer onto blank paper, film, or other record. Federal Information Resources Management Regulation Bulletin B-3 defines electronic form: "Like a photocopy, an electronic reproduction must be complete, containing all instructions and questions which appear on the current official form. The wording and punctuation of all items, instructions, and identifying information must match exactly. No data elements may be added or deleted. The sequence and format for each item on the form must be reproduced to the highest degree possible. Each item must print on the same page in approximately the same position. However, forms printed face and back on the original may be printed on single sheets provided each page is identified with form number, page number, and edition date. Likewise, multiple part sets may be printed as single sheets. The final form must be printed using the same dimension as the current edition is printed. All blocks must remain approximately the same size and lines must remain approximately the same size length. The electronic form should contain the software name and vendor/producer (if any) at the bottom of the face page."

Electronic Interoperability—A special form of interoperability where two or more electronic equipment, especially communications equipment, can be linked together, usually through common interface characteristics and so operate the one to the other. See also Interoperability.

Electronic Mail (E-mail)—1. The information exchanged between individuals or organizations by means of application of computer-to-computer data transfer technology, normally as textual messages. 2. Communication processed through a network, from one workstation to another.

Electronic Printing—Electronic composition, reproduction, and finishing of information for general distribution produced through high-speed imaging without a plate, using nonimpact methods on paper, film, magnetic, or optical media.

Electronic Private Branch Exchange (EPBX)—Provides the same services as a private branch exchange but with manual operations accomplished by cordless consoles instead of cord-type switchboards. EPBXs are electronic processors controlled with either space-division or time-division switching.

Electronic Publishing—An electronic means for providing all aspects of the document publishing process, including creation, text and graphics design and capture, editing, storage, transfer, printing, and distribution.

Electronic Records—Records stored in a form that only a computer can process.

Electronic Records System—Any information system that produces, processes, or stores records by using a computer. Exceptions: (1) Content Exception. Additions or changes to or deletions of one or more data elements on a form. (2) Electronic Form Exception. An approval to reproduce the image of a form from a stored electronic file of a computer system. An electronic form exception does not authorize the user to change the content or format of the form, but only to reproduce the form electronically. (3) Format Exceptions. Changes made by altering the spacing of a form or rearranging its data elements without changing the data elements themselves. (4) General Exceptions. Approval for an agency or activity to change the content, format, or printing of form. (5) Printing Exceptions. Changes in the printing specifications of a form; that is, changes to the color, size or type of paper, changes in color or type of ink, the establishment of multipart sets and marginally-punched constructions in lieu of cut sheets; and use of an alternative printing technology (e.g., electronically generated forms may require a format exception.

Electronic Warfare (EW)—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within EW are: electronic attack, electronic protection, and electronic warfare support.

Embedded Computer System—A computer system that is integral to a larger system whose primary purpose is not computational. An embedded computer would require major modifications in order to be used for general-purpose computing and is managed as a component of the system in which it is embedded.

Emulator—In computing, special-purpose hardware or software that enables one system to act as if it were another. It is used, for example, to minimize reprogramming efforts when a new computer replaces an existing one.

Encrypt—Convert plain text into unintelligible form by means of a cryptosystem.

End-Fire Array—Antenna An antenna consisting of a linear array of radiators in which the maximum radiation is along the axis of the array; the antenna may be uni- or bi-directional.

End Instrument—A device connected to the terminal of a circuit and used to convert usable intelligence into electrical signals or vice-versa.

End Item—A final combination of end products, component parts, or materials that is ready for its intended use. In the C4 world, a complete communications system can be designated as an end item as well as its subsystems or main components, such as radio transmitters, receivers, antenna system, and so forth.

End Office (EO)—An integral part of the Defense Switched Network (DSN). An EO provides switched call connections and all DSN service features, including multi-level precedence and preemption. The EO provides long distance service by interconnection with multifunction switches. The EO does not serve as a tandem in the DSN, but may connect to other EOs where direct traffic volume requires using a community of interest trunk. As part of the DSN, EOs will be interconnected to and supervised by the DSN system control subsystem.

End User—The individual who operates the computer. The preferred term in the Air Force is **User**.

End-User Devices—Information system terminal components (e.g., workstations, telephones, sensors, displays, and radios) which are used to enter date, extract information, or control processing and transfer; functional end-user organizations generally control these resources.

Engineering and Technical Services—Advice, instruction, and training in the installation, operation, and maintenance of weapon systems, equipment, and components used by DoD components. These services are provided by qualified DoD military and civilian personnel, or by employees of DoD contractors.

Enhanced Telephony—Enhanced telephony environments provide improved means of using the telephone system for interactive audio exchanges between users. Features include: call forwarding, call waiting, programmed directories, teleconferencing capability, automatic call distribution, and call detail recording.

Envelope—In a message handling system, the part of a message that contains information necessary to deliver the message to the recipient. In addition, the envelope may contain information that identifies the message originator and potential recipients, records details of the routing by the message transfer system, and characterizes the message content.

Envelope Delay—In telecommunications, envelope delay refers to the characteristics of a circuit that cause certain frequencies to be delayed more than others resulting in distortion of the overall frequency envelope at the receiving end.

Ephemeris—A table giving the coordinates of a celestial body at a number of specific times during a given period. The term also applies to artificial satellites.

Equalization—The process of reducing frequency distortion and, or phase distortion of a circuit by the introduction of networks to compensate for the difference in attenuation and, or time delay at the various frequencies in the transmission band.

Equalizer Delay—In telecommunications, a corrective network used in a circuit for the purpose of compensating for the phase delay and envelope delay characteristics of the circuit and making these delays substantially constant over the desired frequency range thereby minimizing distortion of the signals.

Equatorial Orbit—For a satellite orbiting the earth, an orbit in the equatorial plane.

Equipment Reliability—The percent of time a specific equipment component was operational during a specified period of time.

Erase—To replace all the binary digits in a storage device by binary zeros.

Erlangb—A unit of telecommunications traffic intensity determined by the product of the number of calls carried by the circuit and the average duration of the call in hours.

Error Correcting Code (ECC)—A code designed to detect an error in a word or character, identify the incorrect bits, and replace them with the correct ones.

Error Rate—The ratio of the number of bits, elements, characters, or blocks incorrectly received to the total number of bits, elements, characters, or blocks transmitted in a specified time interval. Also see **Bit Error Rate**.

Ethernet—A baseband local area network specification developed jointly by Digital Equipment Corporation, Xerox, and Intel to interconnect computer equipment using coaxial cable and transceiver

European Telephone System (ETS)—The military telephone system in Europe that uses digital telephone switches. ETS is part of the Defense Switched Network.

Evaluation—The review and analysis of qualitative or quantitative data obtained from design review, hardware inspection, testing, or operational use of equipment.

Expanded Binary Coded Decimal Interchange Code (EBCDIC)—1. An 8-bit code used to represent 256 unique letters, numbers, and special characters. 2. The standard representation of numbers and letters by IBM computers.

Exterior Gateway Protocol (EGP)—The service by which gateways exchange information about what systems they can reach.

External Environment Interface (EEI)—The interface between the application platform and the external environment across which information is exchanged. The EEI is defined primarily in support of system and application interoperability.

Extraterrestrial Noise—Random noise originating in outer space and detected on the Earth.

Extremely High Frequencies (EHF)—Frequencies of electromagnetic waves ranging from 30-300 gigahertz.

Extremely Low Frequencies (ELF)—Frequencies of electromagnetic waves below 300 hertz.

F—A term used in publishing bulletins meaning Functional Distribution.

Facsimile (fax)—A system of telecommunications for transmitting fixed images (e.g., pictures, drawings, text, etc.) with a view to their reception in a permanent form.

Fading—In radio communications, fluctuations in the strength of received radio signals because of variations in the transmission medium. These variations are generally due to atmospheric, electromagnetic, and/or gravitational influences that cause the radio signals to be deflected or diverted away from the receiving antenna.

Federal Agency—A department, independent agency, commission, or establishment of the Executive Branch.

Federal Benefit Program—A Federally funded or administered program for individuals that provides cash or in-kind assistance (payments, grants, loans, or loan guarantees).

Federal Education Program—Any Federal agency with a primary purpose of offering instruction or affecting an educational agency's or institution's ability to offer instruction.

Federal Information Processing Standards (FIPS)—Issued by the National Bureau of Standards, they announce the adoption and implementation of specific information systems standards and guidelines within the Federal Government.

Federal Printing Program (FPP)—A Joint committee on printing-directed program that regulates printing in the Federal Government. It directs Federal agencies to buy their printing from the Government Printing Office (GPO) or through GPO contracts with commercial printers. It also regulates the work that agencies may produce in-plant printing. The program is designed to contract as much printing as possible from the private sector.

Federal Telecommunications System (FTS)—A general-purpose, nationwide, nonsecure voice communications network managed and operated by the Government Services Administration. It supports the essential needs of Federal Government departments and agencies. The FTS provides local, long-line (intercity), and commercial interface service to its subscribers.

Federated Data Base—A set of cooperating data management facilities (DMF). A DMF is the set of all data management component present on a specific platform. Each DMF makes a portion of its data base available to one or more other members of the federation by making part of its scheme known to the other DMFs.

Femto (f)—A prefix used to denote one quadrillionth (10-15).

Fiber Crosstalk—In opto-electronics, the exchange of light wave energy between the core and the cladding of a fiber optic cable, the cladding and the ambient surrounding, or between different indexed layers. The crosstalk is deliberately reduced by making the cladding loose.

Fiber Distributed Data Interface (FDDI)—A standard of transmitting data on optical fiber cables at a rate of around 100 Megabits-per-second (10 times faster than ethernet, about twice as fast as T-3)

Fiber Optics—The technology of using thin glass or plastic filaments to transmit signals as pulses of light at frequencies of about 1014 hertz. The filament acts as a wave guide for the light, reflecting it back and forth from the inside walls, allowing it to be transmitted around bends and over long distances with minimal loss.

Field—The term for an item on a form, such as a name or address. Fields form records in a file or data base.

Figure—Anillustration such as a map, drawing, photograph, graph, or flow chart, or other pictorial device inserted into a publication. Additionally, a figure can also be an illustration that is set in type such as a sample format or memorandum.

File—1. In data structures, a collection of records that are logically related to each other and handled as a unit (e.g., by giving them a single name). 2. A grouping of data in a named entity, under a file name, organized into special, ordinary, or directory files. 3. In electronic recordkeeping, an organized collection of related data, usually arranged into logical records that are stored together and treated as a unit.

File Allocation Table (FAT)—In computing, a table used by the operating system to allocate space on a magnetic disk for a file. The sectors allocated may be randomly scattered over the disk and the table locates and chains together the sectors for each file.

File Format—In computing, the structure or arrangement of data stored in a file. Applications always store data files in a particular format. A format readable by one application may not be readable by another.

File Server—1. A computer with connectivity to more than one user, used as a centralized information storage device. This system allows users to exchange data, applications software, and files. The file server may have software packages for electronic mail, calendars, system administration, and so forth. 2. The file server provides transparent access to files from workstations and other clients. Unlike a data server, the file server provides access and linkage to the file directories and is not aware of the contents of the file. Processing of the contents of the file needs to be performed by the client. The file server does no client visible manipulation of the data within a file. Essentially, the file server provides the client with the use of a virtual disk drive and little else. In a workstation environment, the workstation would perform all the processing on the file.

File Transfer Protocol (FTP)—A Transmission Control Protocol/Internet Protocol application program used to transfer files from one computer to another. It is commonly used on the Internet.

Filter—An electrical or electronic device or network that passes desired frequencies, but blocks or greatly attenuates others. There are two basic types, active and passive filters. Active filters require the application of electrical power for the utilization of their filtering properties, passive filters do not.

Firewall—1. A protection scheme that assists in securing internal systems from external systems. 2. In data communications systems, a type of router that is placed between a network and the internet to selectively filter incoming and outgoing traffic. Firewalls enhance network security.

Firmware—Software that is permanently stored in a hardware device that allows reading but not writing or modifying the software. The most common device used for firmware is read-only memory.

First Generation Language—In programming, a machine code or assembly language.

First In-First Out (FIFO)—An algorithm used in determining the order of handling or consideration. At any one time, the next item to be dealt with is that item among a group of items that has been waiting the longest. It is the inherent structure of a queue.

Five-Year Interoperability Assurance Plan (FYIAP)—A Joint Chiefs of Staff (JCS) program managed by Joint Interoperability Test Center (JITC) that documents requirements for C4 interoperability certification, recertification, requalification, and revalidation testing. The FYIAP, published annually in January, establishes the C4 interoperability testing and certification program: FYIAP preparation is tied to the planning, programming, and budgeting system cycle. DoD components identify requirements for testing. JITC consolidates and sends the requirements to the JCS for validation approval. The FYIAP identifies the resources required to support testing during the acquisition process and thereafter, as needed.

Flagship Periodicals—Air Force Recurring Periodical 35-1, *Airman Magazine*, is the premier periodical of the United States Air Force. It contains official and unofficial statements of service officials; news and features on service policies, programs, missions, and personnel; and articles covering major themes of relevance to the United States Air Force.

Flexible, Modular C4 Packages—Flexible, modular C4 packages consist of compatible and interoperable hardware, software, and data base modules and appliquÈs. Examples include rugged, lightweight, small hardware for mobile and transportable use; easily configured shelters and equipment for start-up, operation, and removal.

Font—A family, set, or particular assortment of consistent size, shape, or style of print characters.

Footprint—That portion of the Earth's surface illuminated by a narrow radio frequency signal beam from a satellite and less than Earth coverage.

Format—1. Arrangement of bits or characters within a group, such as a word, message, or language. 2. Shape, size, and general make-up of a document. 3. A guide, table, sample, or exhibit that illustrates a predetermined arrangement or layout for presenting data. A format may or may not be a form.

Forms—A form is a predetermined arrangement of captioned spaces, developed for collecting, recording, and extracting information in a standardized order. The form may exist on paper or film negative, be programmed in computer language, or displayed on a video terminal.

Formula Translator (FORTRAN)—A high-level programming language initially designed for scientific applications, but now used for many commercial and industrial applications.

FORTEZZA—The name given to the Personal Computer Memory Card International Association card used in the encryption and authentication of defense message system messages.

Fortuitous Conductor—Any conductor that may provide an unintended path for electrical signals (e.g., water pipes, metallic structural members, etc.).

Forward Error Correction—The use of an error-correcting code to automatically correct some or all of the signals detected as being in error before they arrive at the data sink.

Forward Scatter—Radio wave propagation in which the direction of the incident wave and the scattered wave lie in or near a great circle plane containing the transmit and receive antennas. The term scatter can be applied to reflection or refraction by relatively uniform media, but is usually taken to mean propagation in which the wavefront and direction are modified in a relatively disorderly fashion.

Four-Wire Circuit—A two-way circuit using two paths so arranged that the electrical signals are transmitted in one direction only by one path and in the other direction only by the other path.

Fourth-Generation Language—A computer programming language (of an order higher than high-order programming languages) designed for easy use by personnel with minimal data processing experience or training to retrieve information from an existing computer application system or quickly develop application software systems or portions of software systems.

Frame Frequency—The number of times per second a frame of information is transmitted or received.

Frame Relay—A packet mode service, a network access protocol for bursty data applications. It is a standard interface specification optimized for transport protocol-oriented traffic. Frame relay can improve on other protocols, such as X.25, local area network bridges, and routers, and help further optimize network resources.

Frame—1. A single display image or screen on a monitor. 2. In a time division multiplexing system, a frame is a repetitious group of signals resulting from a single sampling of all channels, and including any additional signals for synchronization and other required system information.

Framing Bit—A bit at a specific recurring interval in a bit stream used to denote the beginning or end of a frame (a predetermined group of bits). A bit used for frame synchronization. In a bit stream, framing bits are noninformation bits.

Free Space—Empty space with no free electrons or ions present. The term also implies remoteness from material objects that could cause reflection of radio waves.

Frequency—The number of cycles per unit of time. In electrical/electronic applications, the measurement unit of a frequency is the hertz that is one cycle per second.

Frequency Allocation—The designation of frequency bands for use in performing specific functions or services.

Frequency Allotment—The designation of specific frequency bands or frequencies, within a prescribed allocation, for use by a certain country or organization, or within certain areas.

Frequency Assignment—The process of designating a specific frequency for use at a particular station for specified operating conditions.

Frequency Deconfliction—A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management.

Frequency Deviation—In frequency modulation, the peak difference between the instantaneous frequency of the modulated wave and the carrier frequency.

Frequency Diversity—A method of diversity transmission and reception whereby the same information signal is transmitted and received simultaneously on two or more independently fading carrier frequencies.

Frequency Division Multiple Access (FDMA)—In satellite communications, the use of frequency division to provide multiple and simultaneous transmission to a single transponder.

Frequency Drift—A slow, undesired change in the frequency of an oscillator (in a transmitter or receiver).

Frequency Hopping—In radio communications, the periodic changing of the frequency or frequency set associated with a transmission. Successive frequency sets are determined by a pseudo noise code. A frequency hopping signal may be regarded as a sequence of modulated pulses with carrier frequencies that hop in a pseudo random pattern. The net effect is to spread the information over a wider bandwidth, thereby reducing the effects of jamming or interfering signals.

Frequency Modulation (FM)—In radio communications, the form of angle modulation in which the instantaneous frequency of the sine wave carrier is caused to depart from the carrier frequency by an amount proportional to the instantaneous value of the modulating signal.

Frequency Shift Keying (FSK)—A form of frequency modulation in which the modulating signal shifts the output frequency between predetermined values and in which the output signal has no phase discontinuity.

Frequency Spectrum Management—The function where use of the radio frequency spectrum is controlled to ensure the electromagnet compatibility of communications-electronics systems. Requirements for use of the radio frequency spectrum are presented, reviewed, and, to the degree possible satisfied for communications-electronics systems being acquired or brought into use.

Frequency Tolerance—The maximum permissible departure by the center frequency of the frequency band occupied by an emission from the assigned frequency, or by the characteristic frequency of an emission from the reference frequency.

Frequency Translation—The transfer en bloc of signals occupying a definite frequency band (such as a channel or group of channels) from one position in the frequency spectrum to another, in such a way that the arithmetic frequency difference of signals within the band is unaltered.

Front-End Processor—1. A programmed-logic or stored program device that interfaces data communications equipment with an input/output bus or memory of a data processing computer. 2. In a computer network, a processor that relieves a host computer of processing tasks such as line control, message handling, code conversion, and error control.

Front-to-back Ratio—A ratio of parameters used in connection with antennas, rectifiers, or other devices in which signal strength, resistance or other parameters in one direction (of signal or current flow) is compared with that in the opposite direction. The resultant figure is an indicator of the electrical performance of the device.

Full Duplex (FDX) Circuit—A circuit that permits simultaneous transmissions in both directions.

Full Operational Capability (FOC)—The full attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, which is manned and operated by a trained, equipped, and supported military unit or force.

Functional Area Records Manager (FARM)—The FARM is the point of contact and monitors the Records Management Program within his or her functional area.

Functional Design Authority (FDA)—The final authority on a specific software and computer system assigned based on the designated requirement. The FDA is the advocate for all requirements for all users of the system. Only one FDA will be authorized for system approval and functional accountability in each of the 11 established functional domains (i.e., organizations).

Functional Economic Analysis (FEA)—A structured proposal that serves as the principal part of a decision package for enterprise leadership. It includes an analysis of functional process needs or problems; proposed solutions, assumptions, and constraints; alternatives; life-cycle costs; benefits and, or cost analysis; and investment risk analysis.

Functional Model—A structured representation of the activities and functions performed by an organization and the information exchanged between them. This is a portion of architecture.

Functional Publication Library (FPL)—A unit or staff office library that contains only the publications needed for the mission in a specific functional area.

Fundamental Frequency—In a complex, repetitive waveform, the repetition frequency of one cycle of this waveform.

Fusion—C4I for the Warrior fusion is the process of receiving and integrating all-source, multimedia, and multiformat information to produce and make available to the warrior an accurate, complete, and timely summary of essential information required for successful prosecution of operational objectives. Fused information is more valuable to the warrior than information received directly from separate, multiple sources to the degree that it provides the warrior with the real truth.

Fuzzy Logic—In mathematics, a form of logic in which the variables may assume a continuum of values between 1 and 0. All computers operate on a yes or no principle. Simply put, fuzzy logic is a software program that adds a maybe to the process that allows software to operate at a higher level of abstraction and handle conflicting commands.

G/T—In satellite communications, the ratio of antenna gain to noise temperature; it is used to characterize the ground station.

Gain—1. In electronics, the ratio of output current, voltage, or power-to-input current, voltage, or power, respectively. Gain is usually expressed in decibels. 2. The degree to which the strength of a signal is increased when it passes through an amplifier, repeater, or antenna.

Galactic—In data bases, pertains to data that is extensive and accessible from many places and by many applications.

Galactic Noise—Radio-frequency electromagnetic signals originating in outer space.

Garbage In, Garbage Out (GIGO)—A phrase describing the observation that the output of a data system can be no more correct than data it receives as input.

Garble—An error in transmission, reception, encryption, or decryption that changes the text of a message or any portion thereof in such a manner that it is incorrect or undecryptable.

Gateway—1. In data communications, equipment used to interface networks so that a terminal can communicate with a terminal or computer on another network. 2. A device for providing interconnection between networks with different communications protocols; a gateway converts one network's message protocol to the format used by another network's protocol. It can be implemented in hardware or software.

Generic Application Environment (GAE)—One of three technology architecture building blocks. Describes types of information technology application and tools needed to support specific application systems. This is the primary building block in linking application systems back to the technology environment.

Generic Technology Platform (GTP)—A term used to describe the different types of delivery components that can be used to support information technology applications.

Geographical Information System (GIS)—A combination of digital mapping and data base technology that allows the user to see data about items on a map. Commonly used to identify communications circuits or utilities of a given area (e.g., Air Force base). By clicking on a representation of a physical object, such as a building, the user can access progressively greater levels of detail about the facilities within the building, down to circuit or telephone numbers and their actual locations.

Geostationary Orbit—In satellite communications, a circular orbit of 42,242 kilometers' radius that lies in the plane of the equator. A satellite in its orbit appears to remain stationary to an observer on the ground.

Geosynchronous Orbit—In satellite communications, a circular orbit of 42,242 kilometers' radius that does not lie in the equatorial plane. A satellite in this orbit will have the same period of rotation as the Earth, but the inclination of the orbit, to the equatorial plane, means that to an observer on the Earth's surface the position of the satellite changes with time.

Giga (G)—Prefix used to denote one billion (109).

Global Command and Control System (GCCS)—An automated information system designed to support deliberate and crisis planning with the use of analytic tools and flexible data transfer capabilities. When fully implemented, GCCS will be the single global C4I system to support forces for joint and combined operations throughout the spectrum of conflict. As part of the C4I for the Warrior concept, GCCS evolves into the global, seamless infosphere capable of providing the warrior's fused information requirements.

Global Control Center (GCC)—The Defense Information Systems Agency global facility in Arlington, VA, that provides technical control and monitors the system network integrity of the defense information infrastructure.

Global Grid—The communications structure that moves information through an intergated and interoperable worldwide network of information technology products and management services. It is a mission enabler that provides network-centric connectivity supporting all Joint and Air Force command and control operations and mission support functions. The Global Grid provides the communications connectivity utility enabling Air Force warriors to collect, process, and distribute relevant voice, data, imagery, telemetry, and sensory information to all Air Force and DoD locations; fixed, airborne, and deployed. It is the seamless and interoperable infrastructure which integrates the common user networks for in-garrison and deployed forces with sensors, platforms, intelligence systems, space systems, command organizations, and logistics support center to gain full information superiority and dominant battlespace awareness in times of peace and war.

Global Information Infrastructure (GII)—The worldwide interconnection of communications networks, computers, data bases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of communications and information equipment, systems, and networks, to include the personnel who make decisions and handle the transmitted information.

Glomar Response—A reply made to a Freedom of Information Act request that neither confirms nor denies the existence or nonexistence of requested records.

Government Information Locator Service (GILS)—An automated on-line card catalog which identifies public information resources throughout the U.S. Federal Government, describes the information available in those resources, and provides assistance in obtaining the information.

Government-Off-The-Shelf (GOTS)—1. An item of hardware or software that has been produced by or for the government and is available for reuse. 2. Products for which the government owns the data rights, that are authorized to be transferred to other DoD or U.S. Government customers, and that require no unique modifications or maintenance over the life cycle of the product.

Government Printing and Binding Regulations (GPBR)—GPBRs are issued by the Congressional Joint Committee on Printing.

Government Printing Office (GPO) Regional Printing Procurement Office—(RPPO) The GPO is the primary source of Federal printing and is managed by the Public Printer. The RPPOs are established by the Public Printer to buy Federal printing in their areas.

Grams Per Square Meter (g/m2)—The metric equivalent of basis weight for printing materials. It is the weight in grams of one sheet, 1 square meter in size.

Graphical User Interface (GUI)—A system design that allows the user to affect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (e.g., menus, screens, buttons, and so forth).

Graphics Adapter—An item of electronic hardware in a computer that controls the monitor. Also known as a Video Controller.

Ground—In communications-electronics, a conducting connection, whether intentional or accidental, by which an electric circuit or equipment is connected to the earth (ground) or to some conducting body of relatively large extent that serves in place of the earth.

Ground Mobile Forces Satellite Communications (GMF SATCOM)—A multi-service program comprised of ground terminals that are characterized by ease of set-up for quick reaction, transportability, and flexibility of communications links. Provides critical multi-channel command and control transmission requirements between command echelons and the war-fighters.

Ground Potential—Having the same electrical potential as the Earth.

Ground Return Circuit—A circuit in which the Earth serves as one conductor.

Ground Wave—A radio wave that is propagated over the surface of the Earth and ordinarily is affected by the presence of the ground (terrain) and, to a lesser extent, the lower atmosphere.

Groupware—Software and systems that help groups coordinate and communicate about work on which they are cooperating. Groupware may incorporate e-mail, shared data bases, workflow software, conferencing software, and scheduling software.

Guard Band—A narrow band of frequencies left vacant between allocated channels that is intended to minimize the possibility of mutual interference.

Half Duplex Circuit—A circuit that affords communications in either direction, but only in one direction at a time.

Handshaking—Passing control characters between two devices to control the flow of information between the devices.

Hard Disk—A mass-storage magnetic medium that uses a rigid material disk for mass storage of data. Usually hard-disk systems are faster and can store many times more data than is possible on floppy disks of the same physical size. Usually, the disk itself, along with the read/write head, is housed in a sealed enclosure to ensure against contamination. For some systems, hard disks are available as removable cartridges. Under appropriate conditions, the cartridge disks can be used for classified processing in a normal office environment.

Hard Metric—The use of metric (SI) measurements in specifications, supplies, standards, and services.

Hardware—The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. 2. In data automation, the physical equipment or devices forming a computer and peripheral components. See also Software.

Hardware Architecture—Assemblage of a computer's internal components and its attached peripheral devices that determine its capability and its limitations.

Harmful Interference—Any emission, radiation, or induction that endangers the functioning of a radio navigation service or other safety services or which seriously degrades, obstructs, or repeatedly interrupts a radio communication service.

Helios Noise—Interference to satellite communications caused by the sun when an orbiting satellite passes between the sun and a tracking ground station.

Hecto (h)—A prefix denoting one hundred (102).

Hertz (Hz)—A unit of frequency equal to one cycle per second.

Heterochronous—A relationship between two signals such that corresponding significant instants do not necessarily occur at the same time. See also Mesochronous and Plesiochronous.

Heuristic—1. Procedures that are designed to develop a plan or program that will obtain desired results or output as an improvement over current procedures. 2. A term applied to a problem solving technique in which experiences, guesses, and trial-and-error methods are used.

High Bit Rate Digital Subscriber Line (HDSL)—A new technology that extends the distance a T1 (1.544 Mbps) link can operate over copper wire before it requires a repeater to maintain signal integrity. This technology also boasts optical fiber quality bit error rates.

High Frequency (HF)—Frequencies of electromagnetic waves in the range of 3 MHz to 30 MHz.

High Level Data Link Control (HDLC)—A communications protocol defined for high-level, synchronous connections to X.25 packet networks. Similar in most respects to synchronous data link control. See also Synchronous.

High Level Language—Computer programming language that does not reflect the structure of any one computer or class of computers.

High-Order Programming Languages—Programming languages (of an order higher than assembly languages) designed for easy expression of a class of problems or procedures to achieve varying degrees of machine independence. These languages are designed for programming convenience rather than for easy generation of machine code instructions. The languages are intended to present procedures to an interpreter or compiler, which creates a machine language program or series of subroutines for a computer to execute.

High Speed—A term applied to a data communications device or facility capable of handling more than 4,800 bits per second.

Highway—1. A major data transfer path within a computer or other functional unit. It typically consists of a number of wires or multi-conductor cable. Compare to trunk or bus. 2. A digital serial-coded bit stream with time slots allotted to each call on a sequential basis.

Historical (Transaction) File—1. A file containing relatively transient data, that, for a given application, is processed together with the appropriate master file. 2. A file of accumulated data from previous transactional updates the office of primary responsibility (OPR) keeps separately for historical purposes. A valid file of items the OPR uses with the master data input file to create a master data output file. A file identical in format and content to a master file, that the OPR keeps separately for security backup, historical, or similar purposes.

Historical Reference Publications—Publications kept by historians for reference and research.

Homochronous—The relationship between two signals such that their corresponding significant instants are displaced by a constant interval of time.

Hop—In radio communications, the excursion of a radio wave from the Earth to the ionosphere and back to the Earth. The number of hops indicates the number of reflections from the ionosphere.

Horizontal and Vertical C2—The capability for the warrior to communicate and exchange pertinent information up, down, or laterally with any other warrior or organization using any desired form of communications appropriate for effective coordination (e.g., voice, data, video, or integrated mode).

Host—Any computer on a network that is a repository for services available to other computers on the network.

Hot Standby—In reliability, a method of hardware backup where the back-up equipment is under power and is (generally automatically) switched into the system when the primary operating equipment experiences a failure.

Human-Computer Interface (HCI)—HCI encompasses interactions between the user and the system, including controls, displays, environmental concerns, workspace layout, procedures, and documentation. HCI encompasses the look and feel of the interface, physical interaction devices, graphical interaction objects, alternate interactions (voice, touch screen, pen) environmental factors, and any other human-computer interactive methodology.

Human Factors Engineering (HFE)—An approach that makes use of scientific facts in the design of items (i.e., computer systems, software, and so forth) to produce effective human-machine integration and utilization.

Hybrid—In communications-electronics, a functional unit in which two or more different technologies are combined to satisfy a given requirement, combining the advantages of both into one system, such as an electronic circuit having both vacuum tubes and transistors, or a computer designed with both analog and digital characteristics.

Hybrid Coil—In telecommunications, a device designed to convert between 2-wire and 4-wire communications circuits. Synonym: Hybrid Transformer, Bridge Transformer.

Hybrid Coupler—In an antenna system, a hybrid junction used as a directional coupler.

Hybrid Spread Spectrum—In radio communications, a combination of frequency hopping spread spectrum and direct-sequence spread spectrum.

Hypermedia—Computer-addressable documents that contain pointers for linking to multimedia information such as text, graphics, video, or audio in the same or other documents. **NOTE:** The use of hypertext links is known as navigating.

Hypertext—1. The system of coding used to create or navigate hypermedia documents in a nonsequential manner. 2. Textual data stored in a network of nodes connected by links so that it can be accessed directly in a nonsequential manner. These links may reflect relationships not apparent on linear text. The operation of the World Wide Web relies mainly on hypertext as its means of interacting with users. Hypertext is basically the same as regular text with an important exception, it contains connections within the text to other documents.

HyperText Markup Language (HTML)—The standard language the World Wide Web uses to create and recognize hypermedia documents. Web documents are typically written in HTML and are usually named with the suffix **.**htm. HTML documents are standard 7-bit ASCII files with formatting codes that contain information about layout (text styles, document titles, paragraphs, etc.) and hyperlinks.

HyperText Transfer Protocol (HTTP)—The protocol for moving hypertext files across the internet. Requires an HTTP client program on one end, and an HTTP server program on the other end.

Icon—Graphical representation of an object, concept, or message used by a computer system to represent items such as files, documents, programs, and disk drives.

Idle-Channel Noise—In telecommunications, random noise signals that are present in a communications channel when no intelligence signals are applied to it. The conditions and terminations must be stated for the noise measurements to be meaningful. Also see Noise.

Image—The picture stored on paper, as lines and characters on a video display tube, or as an electronic image encoded in magnetic or optical media.

Image Formation Time (IMF)—The time required to update screen image displays.

Image Frequency—In frequency heterodyning, an undesired input frequency that is capable of producing the same output frequency (intermediate frequency) that the desired input frequency produces.

Imagery—Collectively, the representation of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

Impedance—In electronics, the total passive opposition of an electronic circuit, device or component to the flow of an alternating current through the circuit, device, or component.

Implementation—1. Procedures governing the mobilization of the force and the deployment, employment, and sustainment of military operations in response to execution orders issued by the National Command Authorities. 2. The publication by the DoD components of directives, instructions, regulations, and related documents that define responsibilities and authorities and establish the internal management processes necessary to carry out the policies required by DoD issuances.

Impulse Noise—Noise consisting of random occurrences of energy spikes, having random amplitudes and bandwidths, whose presence in a data channel can be a prime cause of errors.

Impulse—A surge of electrical energy, usually of short duration and of a nonrepetitive nature.

In-Band Signaling—In telecommunications, signaling that uses frequencies or time slots within the bandwidth of the information channel.

In-Circuit Emulator (ICE)—A combined hardware and software system that enables a prototype microprocessor system to be tested.

In-Line Image—In networking, a graphic image that is displayed with an hypertext mark-up language (HTML) document.

In-Phase—In electronics, pertaining to signals that have zero phase shift relative to each other. Compare Out-of-Phase.

In-Plant System—Synonymous with In-House System.

Inclined Orbit—The orbit of a satellite that is neither equatorial nor polar.

Independent Sideband Transmission—That method of double sideband transmission in which the information carried by each sideband is different (the carrier may be suppressed).

Indexing—The process used to identify a document, specific images, or data elements for retrieval purposes.

Information—1. Any communications or representation of knowledge such as facts, data, or opinions, in any medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. 2. Unprocessed data of every description which may be used in the production of intelligence. 3. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Appliance—A communications device which connects to the information utility to make information available to the user. Examples are: telephones, facsimile machines, desktop computers, network hubs, servers, etc.

Information Assurance—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Attack—An activity taken to manipulate or destroy an adversary’s information without visibly changing the physical entity within which it resides.

Information-based Processes—Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. Information-based processes may be found in any facet of military operations, from combat through combat support and combat service support across the range of military operations.

Information Bit—A bit that is generated by the data source and delivered to the data sink and which is not used by the data transmission system.

Information Collection—1. Internal. Internal information collection is data or information that is systematically collected and formatted by one or more organizational elements and vertically transmitted to another organizational element to meet an authorized and formally specified management information requirement. This includes onetime requests. 2. Interagency. An interagency reporting requirement is data or information that is transmitted between Federal agencies for use in determining policy; planning, controlling, and evaluating operations and performance; making administrative decisions; or preparing other reports. 3. Public Use. A public-use information collection (or reporting requirement) is an information requirement imposed on the public. It is the soliciting of information by a Federal agency from 10 or more respondents, whether such collection of information is mandatory, voluntary, or required to obtain a benefit.

Information Collection Budget (ICB)—The Federal Government’s projected burden on the public for new requirements to collect information. It is the estimated response time (direct and indirect) for the public to collect, record, and submit information to the Federal Government. Each year the Office of

Management and Budget issues a budget call for the Federal Government's ICB.

Information Dominance—1. That degree of superiority in information functions that permit friendly forces to operate at a given time and place without prohibitive interference from opposing forces. 2. A condition in which a nation possesses a greater understanding of the strengths, weaknesses, interdependencies, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the adversary has of that nation.

Information Engineering—1. An integrated and evolutionary set of tasks and techniques that enhance business communication throughout an enterprise enabling it to develop people, procedures, and systems to achieve its vision. 2. A formal software engineering methodology that covers the complete information system life cycle from organization mission to application software and data base development and maintenance.

Information Environment—The aggregate of individuals, organizations, or systems that collect, process, or disseminate information using any medium or form, including the information itself.

Information Flow—The movement of information from its source to the user, including all handling, processing, and transfers that enable its movement.

Information Integrity—The states that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Information-in-warfare (IIW)—Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global

navigation and positioning, weather, and communications capabilities.

Information Life Cycle—The stages through which information passes, typically characterized as creation or collection, processing, disseminating, use, storage, and disposition.

Information Management (IM)—The planning, budgeting, manipulating, and controlling of information throughout its life-cycle.

Information Model—1. A term used to describe the information resources of the organization and their interrelationships. It is used to support data modeling and resulting data base and document storage design requirements. It provides the information resource managers' views of the architecture. 2. A model that represents the processes, entities, information flows, and elements of an organization and all relationships between these factors.

Information Munitions—In information warfare, software programs or logic elements designed to affect an adversary's information systems.

Information Operations (IO)—1. Actions taken to affect adversary information and information systems while defending one's own information and information systems. (*DoD*) 2. Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare. (*USAF*)

Information Processing Equipment—Any electronic hardware used to process, transfer, or display data. Note, however, that radar and radio aids to navigation are not a function of this regulation.

Information Processing Services—A discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

Information Processing Standards for Computers (IPSC)—A standardization area of the Defense Standardization Program. This area relates to computers and data processing devices, equipment and systems, including, but not limited to character recognition typers, input/output media, formats and labels, programming language, computer documentation, flowcharts and terminology, character codes, data communications and input/output interfaces.

Information Protection (INFO PROTECT)—Any measure to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems.

Information Resources—Information and related resources, such as personnel, equipment, funds, and information technology.

Information Resources Management (IRM)—The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burden on the public. The term encompasses both information itself and the related resources such as personnel, equipment, funds, and information technology.

Information Services—A discrete set of information activities typically provided on a reimbursable basis. These activities include analysis, acquisition, test, delivery, operation or management of hardware, software, and communications systems.

Information Standards and Technology (INST)—A standardization area of the Defense Standardization Program. This area encompasses report standards, data exchange format standards, graphic, and imagery constructs. It includes the structure, values, definition, and representation of data that gives it meaning, enhances information sharing and exchange, and facilitates effective decision-making based on a DoD-wide commonality of representation and understanding of specific bits of information. Standard structures and formats include character and bit oriented syntax as well as graphics, imagery, and geographical constructs. These information structures are derived by combining and using standard data elements and codes to convey precise meaning.

Information Superiority (IS)—1. The ability to obtain and transmit information unimpeded to any destination as and when needed and to exploit or deny an adversary's ability to do so. This includes the ability to manage information throughout its life-cycle, i.e., to create, collect, process, disseminate, use, store, and dispose of an unimpeded flow of information while exploiting or denying an adversary's ability to do the same. (*DoD CIO*) 2. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (DODD S-3600.1) 3. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*). 4. The capability to collect, process, and disseminate an uininterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Vision 2010). 5. **NOTE:** The Air Force prefers to cast "superiority" as a state of relative advantage, not a capability, and views IS as: That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. (AFDD 2-5, *Information Operations*).

Information System (IS)—The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Systems Security—The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users (includes those measures necessary to detect document, and counter such threats).

Information Technology (IT)—1. With respect to an executive agency, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is based by the executive agency directly or is used by a contractor under a contract with the executive agency which (a) requires the use of such equipment or contract, or (b) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. 2. IT includes computers, ancillary equipment, software, firmware similar procedures, services (including support services), and related resources. 3. Notwithstanding definitions 1. and 2., IT does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Clinger-Cohen Act of 1996).

Information Technology Standards—Provide technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission or transfer. Information technology standards apply during the development, testing, fielding, enhancement, and life-cycle maintenance of DoD information systems. Information technology standards include nongovernment national or international standards, federal standards, military standards, and multinational treaty organization standardization agreements. They may take numerous forms including standards, handbooks, manuals, specifications, commercial item descriptions, and standardized drawings, all are referred to collectively as Standards.

Information Utility—A provider of access to information services. To the customer the information utility is transparent and appears as an unrestricted transport of information from source to destination.

Information Warfare (IW)—1. Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DODD S-3600.1). 2. Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems (AFDD 2-5).

Infra Low Frequency (ILF)—Frequencies of electromagnetic waves in the range of 300-3000 hertz.

Infrasonic Frequency—A frequency below that of sound waves audible to the human ear. Usually taken as a frequency of 15 hertz.

Infrastructure—1. At the national level, the framework of interdependent networks and systems, comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole. 2. At the base level, the common-user portion of the communications and information systems environment. It includes transmission, switching, processing, system-control and network-management systems, equipment, and facilities that support the base. Examples are the telephone switch and cable plant, base communications center, land mobile radio system, and local area networks.

Infrastructure Asset—Any infrastructure facility, equipment, service, or resource that supports a DoD component. A critical infrastructure asset is an infrastructure asset deemed essential to DoD operations or the functioning of a critical asset.

Initial Distribution (ID)—The first automatic distribution of a new or revised publication, either by a publishing distribution center to a publishing distribution office (PDO), or by a PDO to a customer account representative, against established requirements, or direct to addresses designated by an office of primary responsibility.

Initial Operational Capability (IOC)—1. At the system level, IOC is the point at which some portion of the technical and operational specifications defined by the requirements' documents have been achieved. The specific definition of IOC will vary for each system and would be negotiated between the program manager, the user, and the operations and maintenance (O&M) activity. 2. At the site level, IOC is the point at which the technical specifications of that portion of the system installed at a specific site meet the documented requirements, but some portion of testing and, or operational specifications remains to be accomplished. The specific definition of IOC is site specific and would be negotiated between the program manager, the site manager, and the O&M activity.

Input—Data or signals keyboarded or transmitted into a computer system.

Input/Output Channel—A device that handles the transfer of data between internal memory and peripheral equipment.

Input/Output Device—A device that introduces data into or extracts data from a system.

Inquiry—A request for information from storage (a request for specific information from a stored collection of data).

Inside Plant—All the cabling and equipment installed in a telecommunications facility.

Inside-the-Gate—Collective term for the various components that make up the base communications infrastructure, consisting primarily of the Network Control Center, on-base cabling, and transmission systems.

Institute of Electrical and Electronics Engineers (IEEE)—An accredited standards body that has produced standards such as the network-oriented 802 protocols and portable operating system interface for computer environment (POSIX). Members represent an international cross-section of users, vendors, and engineering professionals.

Integrated Circuit (IC)—In electronics, a combination of interconnected circuit elements inseparable associated on or within a continuous substrate. An IC may contain a few to many thousands of transistors, resistors, capacitors, and diodes.

Integrated Computing—In programming, the concurrent use of data by two or more software packages (e.g., a graphics package that displays spreadsheet data).

Integrated Data Base—A data base of logically integrated entities, relationships, and attributes created after analysis of an information model.

Integrated Optical Circuit—In opto-electronics, the optical equivalent of a microelectronic circuit.

Integrated Services Digital Network (ISDN)—1. ISDN represents a complete network architecture that follows the guidelines of the seven-layered open system interconnection model. The objective of ISDN is to provide a small set of user/network interfaces that give the user standard access to a network or multiple networks. At the user side of the user/network interface, different types of user information (voice, data, and video) are integrated and sent over the standard ISDN transmission line. At the network side of the user/network interface, ISDN provides a single, standard access to diverse services in multiple networks (voice, packet data, video), creating the illusion of a single, ubiquitous network. This eliminates the need for dedicated access to obtain the services available on many networks. 2. An evolving network that will provide end-to-end digital connectivity to support a wide range of services, including voice and nonvoice services, to which users have access by a limited set of standard multipurpose user network interfaces.

Integrated System—A telecommunications system that transfers analog and digital traffic over the same switched network.

Integrity—In data communications, absolute verification that data has not been modified in transmission or during computer processing.

Intelligent Terminal—A terminal containing a microprocessor and is capable of emulating other terminals, validating data, implementing protocols, and so forth.

Interactive—Computer programs that allow performance of several complex functions or operations at the same time, based on response from the operator.

Interactive Courseware (ICW)—Includes all instructional materials and computer software designed and developed for interactive instruction. It refers to an instructional method by which trainees interact individually to training presented through a variety of media controlled and monitored by a computer. The ICW supports informational training, drill and practice, tutorial, simulation, gaming, and problem-solving instructional strategies in a self-paced, stand-alone, or networked training environment.

Interactive Process—A process of calculating a desired result by a repeating cycle of operations that comes closer and closer to the desired result; conversational operation of a computer system using an on-line cathode ray tube terminal.

Interactive Service—In an integrated services digital network, a telecommunications service that facilitates a bi-directional exchange of information among users or among users and hosts. Interactive services are grouped into conversational services, messaging services, and retrieval services.

Interactive Video Disk (IVD)—A desktop, computer-based training system combining an optical laser disk player, microcomputer, and a television monitor. The interaction is achieved by using a touch screen, lightpen, keyboard, or other input device. The user's interactivity is achieved through an operating program specifically designed and authored for each IVD course.

Interagency Report—Data or information transmitted between or among Federal agencies for use in determining policy; planning, controlling, and evaluating operations and performance; making administrative determinations; or preparing other reports. The data or information may be displayed on paper, magnetic tapes, or other media.

Interconnection—The linking together of interoperable systems.

Interface—1. A boundary or point common to two or more similar or dissimilar communications systems, subsystems, or other entities against which or at which necessary information flow takes place. 2. A concept involving the specification of the interconnection between two systems or items of equipment. The definition includes the type, quantity, and function of the interconnecting circuits and the type and form of signals to be interchanged via those circuits. Mechanical details of plugs, sockets, pin numbers, and so forth, may be included within the context of the definition. 3. The process of interrelating two or more dissimilar circuits or systems. 4. A connecting link between two systems. In the open system interconnection reference model, it is the boundary between adjacent layers.

Interference—The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions on reception in a radio communications system, manifested by any loss of information that could be extracted in the absence of such unwanted energy.

Interleaving—1. In digital communications, the transmission of pulses from two or more digital sources in time division sequence over a single path. 2. A technique used in conjunction with error correcting codes to lower the error rates of communications channels characterized by burst errors.

Interlock—To arrange controls of machines or devices so that their operation is interdependent in order to ensure their proper coordination.

Intermediate Language—A language other than machine code that is produced by a compiler as a step in compiling a high-level language program.

Intermodulation—The production, in a nonlinear transducer element, of frequencies corresponding to the sums and differences of the fundamentals and harmonics of two or more frequencies which are transmitted through the transducer.

Intermodulation Noise—In a transmission path or device, (undesirable) noise that is generated during modulation and demodulation and is the result of nonlinear characteristics in the path or device.

Internal Information Collection/Reporting Requirement—Data or information collected by one or more organizational components and transmitted to other organizational components for management purposes. The collections required for management purposes pertain to policy; planning, controlling, and evaluating operations and performance; making administrative determinations; and preparing other reports. It is status, summary, or statistical information in both electronic and manual information systems.

International Organization for Standards (ISO)—An international organization responsible for the development and publication of international standards in various technical fields. It consists of member bodies that are the national standards bodies of most of the countries of the world. The ISO has its headquarters in Geneva, Switzerland. The American National Standards Institute is the representative standards body for the United States.

International Standards—Agreed upon international standards as voted by the International Organization for Standards. (See ISO).

International Telecommunication Union (ITU)—The ITU, with headquarters in Geneva, Switzerland, is an international organization within which governments and the private sector coordinate global telecommunication networks and services. Activities include telecommunications standardization, radio communications, telecommunications development, and organization of telecommunications events. The ITU promotes standardized telecommunications on a worldwide basis. It is recognized by the United Nations Organization as the specialized agency for telecommunications.

Internet—A catch-all term used to describe the massive worldwide network of computers. Literally it means network of networks, and is a worldwide interconnection of individual networks operated by government, industry, academia, and private sectors. Although there is no single governing body that controls the internet, there are companies that help manage different parts of the networks that tie everything together. The networks within different countries are funded and managed locally according to local policies. Access to the internet means access to a number of basic services, such as electronic mail, interactive conferences, access to information resources, network news, and files transfer capability.

Internet Standard—A standard produced by the Internet Architecture Board that identifies one or more internet requests for comment that are required for a given data communications function or internet service.

Intranet—A private network inside a company or organization that uses the same kinds of software as found on the internet, but that is only for internal use.

Interoperability—1. The ability of systems, units, or forces to provide services to and accepts services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between them and, or their users. The degree of interoperability should be defined when referring to specific cases.

Interoperability Standard—A document that establishes engineering and technical requirements that are necessary to be employed in the design of systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together.

Interrupt—A break in the normal flow of a system or routine such that flow can be resumed from that point at a later time.

Intramodal Distortion—In an optical fiber, distortion caused by dispersion, such as material or profile dispersion, of a given propagating mode.

Intrinsic Noise—In telecommunications, in a transmission path or device, that noise which is inherent to the path or device and is not contingent upon modulation.

Intrinsically Safe—The National Electrical Code defines IS equipment as equipment not capable of releasing sufficient electrical or thermal energy to cause ignition of specific flammable or combustible atmospheric mixture in its most ignitable concentration.

Inward-Outward Dialing—A dialing capability where calls are dialed directly to and from base telephone stations without operator assistance. Inward-outward dialing improves speed of service, reduces switchboard operator workload, and lowers operating costs.

Ionosphere—That part of the earth's atmosphere, extending from approximately 70 kilometers to 500 kilometers altitude, where ions and free electrons exist in sufficient quantities to reflect electromagnetic waves.

Ionosphere Sounder—A device that transmits signals to determine the degree of usability of the ionosphere for radio transmissions.

Ionospheric Scatter—The propagation of radio waves by scattering due to irregularities or discontinuities in the ionization of the ionosphere. Synonym: Forward Propagation Ionospheric Scatter.

Isochronous—That characteristic of a periodic signal in which the time interval separating any two corresponding transitions is theoretically equal to the unit interval or to a multiple of the unit interval.

Isotropic Antenna—A hypothetical antenna that radiates or receives equally in all directions. Isotropic antennas do not exist physically, but represent a convenient reference for expressing directional properties of actual antennas.

Jabber Control—In data communications, a facility in a local area network to interrupt automatically transmission of an abnormally long-output data stream.

Jitter—1. In communication-electronics, abrupt and spurious variations in a signal, such as in interval duration, amplitude of successive cycles, or in the frequency or phase of successive pulses. When used qualitatively, the term must be identified as being time, amplitude, frequency, or phase related and the form must be specified. When used quantitatively, a measure of the time or amplitude related variation must be included (e.g., average, root-mean-square, peak-to-peak, and so forth). 2. In computer graphics, a signal instability resulting in sudden, small, irregular variations due mainly to synchronizing defects in the associated equipment. 3. In facsimile, raggedness in the received copy caused by erroneous displacement of recorded spots in the direction of scanning.

Job Control Language (JCL)—In computing, a problem-oriented language used for specifying the environment for running a particular batch of work.

Job-Oriented Terminal—In peripherals, a terminal designed for a particular application.

Joint Communications Control Center (JCCC)—An activity formed at the unified or joint command headquarters with primary responsibility for overall C4 systems management.

Joint Doctrine—Fundamental principles that guide the employment of forces of two or more services in coordinated action toward a common objective. It will be promulgated by the Chairman, Joint Chiefs of Staff, in consultation with the other members of the Joint Chiefs of Staff.

Joint Interface—An interface that passes or is used to pass information between systems or equipment operated by two or more commanders in chief, services, and, or agencies.

Joint Photographic Experts Group (JPEG)—A compression method of storing an image in digital format.

Joint Publications—Publications of joint interest prepared under the cognizance of Joint Staff directorates and applicable to the military departments, combatant commands, and other authorized agencies. It is approved by the Chairman, Joint Chiefs of Staff, authenticated by the Director of the Joint Staff, and distributed through service channels.

Joint Tactical Information Distribution System (JTIDS)—An information distribution system that provides secure integrated communications, navigation, and identification capability for application to military tactical operations. A proposed version of a joint doctrine or joint tactics, techniques, and procedures publication that normally contains contentious issues and is nominated for a test publication and evaluation stage.

Joint Test Publication (JTP)—A draft of a joint doctrine or joint tactics, techniques, and procedures that has evolved far enough in development to be approved for evaluation by the Director, Operational Plans and Interoperability (J-7), Joint Staff. Publication of a test publication does not constitute Chairman, Joint Chiefs of Staff, approval of the publication. Prior to final approval as joint doctrine, test publications are expected to be further refined based upon evaluation results.

Joint Universal Data Interpreter (JUDI)—An integrated software system that provides a fused tactical display of component forces executing on any platform. JUDI is a translator that interprets data formats, parses and analyzes the data, stores the data in a universal Data base, and then formulates the messages for output. It provides interoperability among some major existing command and control systems without the need to modify those systems.

Joint Worldwide Intelligence Communications System (JWICS)—1. The Sensitive Compartmented Information (SCI) portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. 2. A high speed (T-1, 1.544 Mbps) communications system designed to provide secure, system high (TOP SECRET/SCI) data, interactive video teleconferencing, and video broadcasting capabilities to its subscribers.

Journal—1. In communications, a list of all messages sent and received by a terminal. 2. In computing, a chronological record of changes made to a set of data, often used for reconstructing a previous version of the set in the event of corruption.

Judder—In facsimile, an irregular movement of the moving parts in a transmitter or receiver causing straight lines in the source document to be reproduced in a wavy manner.

Jule's Own Version of International Algorithmic Language (JOVIAL)—1. A multipurpose programming language developed for military applications. 2. Class name for a set of programming languages oriented towards command and control usage that are highly distinguishable between each other in commands, scope, and format.

Jumper—1. In electronics, a short wire used for the temporary connection of two points in an electric circuit. 2. A hardware link made within a circuit to select a particular option.

Junction—In electronics, the boundary region between two semiconductors having different electrical properties, or between a metal and a semiconductor. This boundary region is used to control the current flow through a semiconductor.

Justify—In composition, to space out lines of text so that they are of equal length.

Kernel—1. The essential central circuitry that is required to enable a microprocessor to operate (e.g., power supply, the microprocessor itself, clock circuit). 2. A module of a program that forms a logical entity or performs a unit function.

Key—In cryptography, information (usually a sequence of random binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for encrypting or decrypting electronic signals, for determining electronic counter countermeasures, or for producing other keys.

Key Pulsing—A system of sending telephone calling signals in which the digits are transmitted by operation of a push-button key set. The type of key pulsing commonly used is dual-tone multi-frequency signaling; each push button causes generation of a unique pair of tones.

Key Telephone System—In a local environment, terminals and equipment that provide immediate access from all the terminals to a variety of telephone services without attendant assistance.

Keystone Equipment—Includes manufacturing, inspection, or test equipment and is the required equipment for the effective application of technical information and knowledge. Keystone materials have the same significant application.

Kilo (k)—A prefix denoting one thousand (103).

Kilobytes (kb)—One kilobyte equals 1,024 bytes.

Kilohertz (kHz)—A unit of frequency denoting one thousand (103) hertz.

Knife-Edge Effect—The transmission of radio signals into the line-of-sight shadow region caused by the diffraction over an obstacle (e.g., a sharply defined mountain top or ridge).

Ku BAND—In radio communications, the frequency range of 12-18 gigahertz. **NOTE:** Letter designators of radio frequency bands are imprecise and legally obsolete.

L—A term used in publishing bulletins meaning Limited Distribution.

L-Band—In radio communications, the frequency range of 1-2 gigahertz. **NOTE:** Letter designators of radio frequency bands are imprecise and legally obsolete.

Land Line—A colloquial name for conventional telephone services. Land lines include conventional twisted-pair lines, carrier facilities, and microwave radio facilities for supporting a conventional telephone channel, but do not include satellite links or mobile telephone links using radio transmissions.

Land Mobile Radio (LMR)—A radio used to provide local transfer of information by portable, mobile, or base station radios and associated equipment. LMRs include combat deployable radios and base support radios. Radio networks are established on the basis of functional agencies and usually have no connectivity between nets unless more than one net shares a frequency. Each net has its own radio system, antenna, code words, and call signs. The capability does exist for commercial encryption, but this system provides only privacy and not security.

Land Mobile Station—A mobile station in the land mobile radio service capable of surface movement within the geographical limits of an area, country, or continent.

Language—In programming and communications, a set of characters, conventions, and rules used to convey information.

Language Processor—In programming, a computer or other functional unit for processing programs written in a specified programming language.

Laser—In opto-electronics, light amplification by stimulated emission of radiation. A device that emits lightrays that are in phase, traveling in the same direction, and essentially of the same wavelength (i.e., color). A laser beam does not diverge by a significant amount and maintains a high energy density. Lasers are used in optical signaling devices, high speed printers, fiber optics, and holography.

Laser Printer—A fast, high quality, nonimpact printer. The printing centers around a belt consisting of a polyester film covered with a photosensitive material.

Latency—In a rotating storage device such as a disk or drum, the time required to locate the first bit (or character) in a particular storage location.

Layer—In telecommunications networks and open system architecture, a group of related functions that are performed in a given level in a hierarchy of groups of related functions.

Lead Command—For a communications and information system, the major command or field operating agency assigned as the communications and information system's advocate according to Air Force Policy Directive 10-9, *Lead Command.*

Lead-Time—The elapsed time between the date a requisition is sent to the supplying source and the date the requester gets the requested material.

Least Significant Bit (LSB)—In data structures, the bit that occupies the rightmost position in a binary number.

Least Significant Digit (LSD)—Same as Least Significant Bit.

Legacy Environments—Legacy environments could be called legacy architectures or infrastructures and, as a minimum, consist of a hardware platform and an operating system. Legacy environments are systems identified for phase-out, upgrade, or replacement. All data and applications software that operate in a legacy environment must be categorized for phase-out, upgrade, or replacement.

Legacy System—1. A system that is a candidate for phase-out, upgrade, or replacement. Generally, legacy systems are in this category because they do not meet current standards. Legacy system workloads must be converted, transitioned, or phase out (eliminated). 2. A communications and information system that duplicates the support services provided by the migration system. Legacy systems must be terminated so that all future development and modernization can be applied to the migration system.

Level-of-Effort (LOE)—Effort of a general or supportive nature that does not produce definite end products.

Life Cycle—1. The total phases through which an item passes from the time it is initially developed until the time it is either consumed in use or disposed of as being excess to all known materiel requirements. 2. The period of time that begins when a (communications and information) system is conceived and ends when the system is no longer available for use. Automated information system life cycle is defined within the context of life cycle management in various DoD publications. It generally refers to the usable system life.

Life-Cycle Cost (of a Communications and Information System)—The total cost to the government for a system over its full life including the cost of development, procurement, operation, support, and disposal.

Life-Cycle Management—1. The management of a communications and information system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. 2. A management process, applied throughout the life of an automated information system (AIS), that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS.

Light Emitting Diode (LED)—In electronics, a semiconductor diode that glows when supplied with a specified voltage. LEDs are commonly used as alphanumeric display devices.

Light Emitting Diode (LED) Printer—A device similar in operation to a laser printer, except instead of a moving laser beam it uses light from an array of light-emitting diodes. This device has the advantage of having fewer moving parts than the laser printer.

Light Pen—In peripherals, a light-sensitive device that is shaped like a pen and connected to a visual display unit. The tip of the light pen contains a light-sensitive element which, when placed against the screen, reacts to the presence of a scanning spot of the raster display which enables the computer to identify the location of the pen on the screen.

Line—In communications, a device for transferring electrical energy from one point to another, such as a transmission line or a communications channel.

Line Access Protocol (LAP)—In data communications, a data link layer protocol that is a subset of high-level data link control and is used in X.25-based networks.

Line Driver—A digital amplifier used to enhance transmission reliability over extended distances.

Line Replaceable Unit (LRU)—A module, subassembly, or printed circuit card within or attached to an item of communications equipment or computer, which can be replaced without soldering.

Line Transient—In communications, an unwanted voltage pulse of very short duration, which can often produce errors in digital circuits that are not designed to minimize the effects of such interference.

Line-of-Sight (LOS) Propagation—Radio propagation in the atmosphere which is similar to light transmissions in that the radio waves in the very high frequency and above ranges tend to travel as a beam in a straight line between the transmitting and receiving antennas. The intensity of the radio beam decreases mainly due to energy spreading according to the inverse-distance law.

Lines Per Minute (LPM)—In peripherals, a measure of the speed of a line printer.

Link Orderwire—A voice or data communications circuit that (a) serves as a transmission link between communications facilities interconnected by a transmission link, and (b) is used for coordination and control of link and traffic activities.

Link—1. A general term used to indicate the existence of communications facilities between two points. 2. A portion of a circuit designed to be connected in tandem with other portions. 3. A radio path between two points (radio link). The term link should be defined or qualified when used. It is generally accepted that the signals at each end of the link are in the same form.

Liquid Crystal Display (LCD)—A display manufactured from two glass plates sandwiched together with a special fluid. When a voltage is applied, the light polarization in the liquid changes and the image becomes visible through a polarizing filter.

Liquid Crystal Display (LCD) Screen—A form of flat-screen visual display unit employing liquid crystal displays. It is lighter and much flatter than a cathode ray tube type display, requires very little electrical power to operate, and generates very little heat.

Load—1. To fill the internal storage of a computer with information from auxiliary or external storage. 2. The (electrical) power consumed by a device or circuit in performing its function. 3. An power-consuming device connected to an electrical circuit.

Lobe—In radio communications, an identifiable segment of an antenna radiation pattern; a lobe is characterized by a localized maximum signal strength bounded by identifiable nulls.

Local Area Network (LAN)—A telecommunications system, within a specified geographical area, designed to allow a number of independent devices to communicate with each other over a common transmission topology. LANs are usually restricted to relatively small geographical areas (i.e., rooms, buildings, or clusters of buildings) and utilize fairly high data rates. Depending on the implementation, these communications networks can provide internal interchange of voice, data, graphics, video, or other forms of electronic messaging.

Local Reproduction Authorized (LRA)—A form that is reproduced locally. Stock is not available from the order sources.

Log Periodic Antenna—A broadband, multi-element, unidirectional, narrow-beam antenna whose frequency response characteristics are repeated at equally spaced frequencies, with the period equal to the logarithm of the ratio that determines the length and spacing of the elements.

Logical Data Model—A model of data, derived from the functional model, used to develop data bases and software solutions.

Logistics Support—1. Logistics support encompasses the logistic services, materiel, and transportation required to support the continental United States-based and worldwide deployed forces. 2. The composite of all considerations necessary to assure the effective and economical support of a system throughout its programmed life cycle. Included are: supply support, maintenance planning, test and support equipment, transportation and handling, personnel and training, facilities, data and software.

Long-Haul Information Transfer—Information transfer elements that provide for inter-base and both intra- and inter-theater information flow between gateways to other information transfer components; information systems organizations control these resources.

Long-Haul Telecommunications—Communications that permit users to convey information on a worldwide basis. Compared to tactical communications, long-haul communications are generally characterized by higher levels of users (including National Command Authorities), more stringent performance requirements (higher quality circuits), longer distances between users (up to global distances), higher traffic volume and density (larger sizing of switches and trunk cross sections), and fixed or recoverable assets. Normally used in reference to the Defense Information System Network.

Loop—1. The go and return conductors of an electric circuit; a closed circuit. 2. In computer systems, the repeated execution of a series of instruction for a fixed number of times. 3. In telephone systems, a pair of wires from a central office to the subscriber's telephone.

Loop Test—A test that uses a closed circuit (i.e., loop), to detect and locate faults.

Loss—1. The amount of electrical attenuation in a circuit, or the power consumed in a circuit or component. 2. The energy dissipated without accomplishing useful work, usually expressed in decibels.

Low Frequency (LF)—Frequencies of electromagnetic waves in the range of 30-300 kilohertz.

Low Level Language—A language designed to facilitate the writing of efficient programs that execute rapidly with minimum main storage space. They are designed for programming computers of particular makes and models. A low level language may also be termed a computer-oriented language.

Low Level Protocol—In data communications, a protocol that is concerned with the mechanics of communication within a network.

Low-Noise Amplifier (LNA)—In communications-electronics, an amplifier designed to minimize the noise introduced in the early stages of amplification, especially where very weak incoming signals are concerned. An LNA is generally used as the first stage of amplification in most wideband radio receiver systems.

Low Pass Filter—In electronics, a frequency-selective network that attenuates signals with frequencies above a predefined value, but passes signals with lower frequencies.

Low Power Communications Device—A restricted radiation device, exclusive of those employing conducted or guided radio frequency techniques, used for transmission of signs, signals (including control signals), writing, images, and sounds or intelligence of any nature by radiation of electromagnetic energy.

Machine Instruction—An instruction that is written in a machine language and can be executed directly by the processor for which it was designed without translation or interpretation.

Machine Language—In programming, a language for programs that can be expressed directly in binary format acceptable to the central processing unit (CPU). All other programming languages (low- or high-level languages) have to be translated into binary machine code before being executed in the CPU.

Machine Readable—Instructions coded so a computer can understand and process them without further intervention.

Macro—In programming, a pre-defined and recorded series of keystrokes that are used later to simplify repetitive tasks.

Macro Language—In programming, the representations and rules for writing macro-instructions.

Macrobend Loss—In fiber optics, the leakage of light caused by a bend in the cable.

Magnetic Core—A configuration of magnetic material that is intended to be placed in a certain relationship to electric currents and whose magnetic properties are essential to its use.

Magnetic Media—The physical substances used by a computer system (analog or digital) upon which data is recorded through the use of magnetic fields.

Mail Server—The mail server provides mail transfer capabilities for a community of users. The basic function is to support the store and forward of interpersonal messages between users. The mail server moves messages based on the contents of the message envelope, not the message's contents. The mail server also manages the users' mailboxes. It can automatically acknowledge delivery to a user's mailbox. The server will support multiform mail transfer (voice e-mail, graphics). In the near future, compound mail documents could be transferred using this server.

Main Distribution Frame (MDF)—The cable racking in a telecommunications facility on which all distribution and trunk cables into a central office are terminated. (The bulky processing units of the early computers resembled the MDF, hence the origin of the term mainframe for a large computer.)

Main Lobe—Of an antenna radiation pattern, the lobe containing the maximum power.

Main Memory—In memory systems, a program addressable, random access store that transfers instructions/data to and from the central processing unit. The main memory also transfers data to and from backing storage and peripherals.

Mainframe—In computing, a term normally applied to a large, general-purpose computer installation serving a major section of an organization or institution.

Maintainability—A characteristic of design and installation that is expressed as the probability that an item will be retained in or restored to a specific condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.

Maintenance—The function of keeping (communications and information) items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Maintenance of software includes anticipating, detecting, and eliminating errors.

Maintenance Concept—A primary factor in determining logistics support requirements for a (C4) system. It delineates maintenance support levels, maintenance responsibilities (organic and/or contractor), supply responsiveness factors, facility utilization requirements, and maintenance environments.

Maintenance Engineering—The application of techniques, engineering skills, and effort, organized to ensure that the design and development of weapon systems and equipment provide adequately for their effective and economical maintenance.

Maintenance Planning—A process that includes all planning and analysis associated with the establishment of requirements for overall support of a (C4) system throughout its life cycle. It begins with the development of a maintenance concept, continues through the accomplishment of logistics support analysis during the design and development phases, procurement, acquisition of support items, and through the customer use phase when an ongoing system capability is required to sustain operations.

Malicious Logic—Hardware, software, or firmware that is intentionally included into an information system for an unauthorized purpose (e.g., virus).

Management Information System (MIS)—An organized assembly of resources and procedures required to collect, process, and distribute data for use in decision making.

Mapping—The electronic process of creating the edits, rules, and algorithms that control the data entry processing for electronic forms.

Master File—The definitive version of a data file in an automated system. The file is long-term, even though the data may change.

Master Publication Library (MPL)—A centralized repository of standard publications.

Matching Agency—The agency that performs a computer match.

Maximum Usable Frequency (MUF)—The upper limit of the frequencies that can be used at a specific time for radio transmission between two points and involving propagation by reflection from the regular ionized layers of the ionosphere.

Meaconing, Intrusion, Jamming, and Interference (MIJI)—Meaconing, intrusion, and jamming are areas of electromagnetic energy transmission classified as intentional or deliberate action by unfriendly countries. Specifically, meaconing is the transmission or retransmission of actual or simulated signals to confuse radio navigation. Intrusion is the intentional insertion of electromagnetic energy into signal transmission paths, with the objective of deceiving operators or causing confusion. Jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic energy with the objective of impairing the use of electronic devices, equipment, or systems. Interference is the radiation, emission, or indication of electromagnetic energy, unintentionally causing degradation, disruption, or complete obstruction of the designed function of the electronic equipment affected. Intent, not effect, is the deciding factor in determining if an event is classified intentional or unintentional.

Mean Power (of a transmitter)—The average power supplied to the antenna transmission line by a transmitter during an interval of time sufficiently long compared with the lowest frequency encountered in the modulation under normal operating conditions.

Mean-Time-Between-Failures (MTBF)—An indicator of expected system reliability calculated on a statistical basis from the known failure rates of various components of the system. The mean operating time between failures during which the item performs as specified. For a particular interval, the total functioning life of a population of an item divided by the total number of failures within the population during the measurement interval. The definition holds for time, cycles, miles, events, or other measure-of-life units.

Mean-Time-To-Repair (MTTR)—The total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.

Media—In telecommunications, the paths along which the signal is propagated, such as wire pair, coaxial cable, waveguide, optical fiber, or radio path.

Medium Frequency (MF)—Frequencies of electromagnetic waves in the range from 300 kilohertz to 3 megahertz.

Mega (M)—A prefix denoting one million (106).

Megabyte (Mb)—In computing, a unit equal to 1,048,576 bytes.

Megacenter—Also called **Defense Megacenter (DMC)**. A DISA/DISA WESTHEM-consolidated computer installation and its supporting organization providing computer processing, data storage, data communications, computer liaison support, and other related services. This includes building, operating, maintaining, and managing a computing and communications capability that supports command, control, business information systems/applications processing, and information transfer requirements; developing, deploying, operating, and maintaining information systems/applications; and providing information services, training, and other operations services.

Megahertz (MHz)—A unit of frequency denoting one million hertz.

Memory—In computing, any facility for holding data. It is often used to describe a computer's main or internal memory.

Memory Dump—In computing, a listing of the contents of a storage device, area, or selected parts of it.

Menu—In computing, a list of options available within a software application.

Meridional Ray—In fiber optics, a ray of light that passes through the axis of the fiber as a result of internal reflection.

Mesochronous—The relationship between two signals such that their corresponding significant instants occur at the same average rate.

Message—Any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication.

Message Switching—A method of operating a communication network where messages are moved from node to node. The message switch at a node must be capable of storing a message, but need not necessarily wait for the whole message to be received before onward transmission.

Meta Principles—Principles that apply to the information technology environment as a whole. They address the organization's position on architecture, migration, and risk management, as well as its orientation to open or proprietary systems.

Metadata—Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.

Metadata Data Base—A system that manages information about data as an enterprise.

Metallic Circuit—A circuit in which metallic conductors are used and in which the ground or earth forms no part.

Meteor Burst Communications—Communications by the propagation of radio signals reflected by ionized meteor trails.

Method of Collection—The mechanism, or method, by or through which an agency conducts or sponsors a collection of information from the public. This does not affect the requirement that the agency obtain and display a currently valid Office of Management and Budget control number on the collection, or the agency's obligation to disclose its estimate of the average burden hours per response. Collections of information may be conducted by mail or through personal or telephone interview, communications via electronic media, automated collection techniques, or any other approach through which the agency may question the respondent.

Micro (mc)—A prefix used to denote one millionth (10-6).

Microbend Loss—In fiber optics, the leakage of light caused by minute sharp curves in the optical cable that may result from imperfections when the glass fiber meets the sheathing that covers it.

Microcircuit—Synonym for Integrated Circuit.

Microcomputer—A computer in which the processing unit is a microprocessor and that usually consists of a microprocessor, a storage unit, an input channel, and an output channel, all of which may be on one chip.

Microfiche—A sheet of film 105 by 148 millimeters (4 by 6 inches), containing multiple micro-images in a grid pattern. It usually contains a heading or title that can be read without magnification.

Microfilm—A fine grain, high resolution film containing an image or images greatly reduced in size from the original.

Microform—A generic form for any form, whether film, video tape, paper, or other medium, containing miniaturized or otherwise compressed images that cannot be read without special display devices.

Micrographics—The science and technology of recording information on, and retrieving it from, microform. It uses photographic techniques or computers to record images on film.

Microprocessor—A central processing unit implemented on a single chip.

Microprogram—A computer program written in the most basic or elemental instructions or subcommands a computer is capable of executing.

Micro—Prefix used to denote one millionth (106).

Microsecond—A unit of time equal to one millionth of a second.

Microwave—A term loosely applied to those frequency wavelengths that are sufficiently short to exhibit some of the properties of lightwaves (i.e., they are easily concentrated into a beam). Commonly used for frequencies from about 1-30 gigahertz.

Microwave Radio Relay Station—A facility, part of a microwave radio telecommunications system, used for the reception and retransmission of microwave radio signals.

Middleware—A layer of hardware/software/communications introduced to interface a variety of workstation products with several incompatible data base servers. The middleware integrates the data environment in a fashion that provides the user with the illusion of one federated data base, despite the incompatibilities between the individual products. Although it is a commercial-of-the-shelf product, middleware systems are typically significant procurement items. It provides an expensive, but possibly cost-effective solution to tying the old with the new in a fashion compliant with the direction of interoperability in the DoD.

Migration System—An existing automated information system (AIS), or a planned and approved AIS, that has been officially designated to support common processes for a functional activity applicable to use DoD-wide or DoD component-wide. Systems in this category, even though fully deployed and operational, have been determined for transitioning to a new environment or infrastructure. A migration system may need to undergo transition to the standard technical environment and standard definitions being established through the Defense Information Management Program, and must migrate toward that standard. In that process it must become compliant with the Reference Model and the Standards Profile. A system in this category may require detailed analysis that involves the total redesign, reprogramming, testing, and implementation because of a new environment and how the users have changed their work methods and processes. The detailed analysis may identify the difference between as is and the to be system.

Military Standard—A document that establishes uniform engineering and technical requirements for military-unique or substantially modified commercial processes, procedures, practices, and methods.

Military Strategic and Tactical Relay (MILSTAR)—A multi-service command and control satellite communications system. It provides worldwide, two-way, anti-jam, survivable, secure voice, teletype, and data communications. The MILSTAR Air Force terminal segment is configured for installation on aircraft, transportable ground shelters, and ground fixed facilities.

Milli (m)—Prefix used to denote one thousandth (10-3).

Millisecond (msec)—One thousandth of a second.

Miniature Receive Terminal (MRT)—A radio receiver using the VLF/LF frequency spectrum. Primarily used for dissemination of Emergency Action Messages to the SIOP tasked forces.

Mission Bit Stream (MBS)—The total of subscriber information bits being passed through a system. This excludes framing, stuffing, control, and service channel bits.

Mission Need Statement (MNS)—A document, prepared by the respective using command or HQ USAF, that identifies an operational deficiency that cannot be satisfied through changes in tactics, strategies, doctrine, or training. A correction of the deficiency normally entails research and development, production, and procurement of a new system or modification of an existing system.

Mnemonic—Word or code symbolic of another word, code, or function.

Mnemonic Symbol—A symbol intended to aid the human memory.

Mobile Service—A service of radio communication between mobile and land stations, or between mobile stations.

Mobile Telephone Switching Office (MTSO)—Acts as the brains of the entire cellular system. It also serves to tie the cellular system to the Public Switched Telephone Network. The MTSO keeps constant track of the affiliation of all active cellular telephones on its system.

Modeling—The application of a standard, rigorous, structured methodology to create and validate a physical, mathematical, or otherwise logical representation of a (C4) system, entity, phenomenon, or process.

Modeling Service Standards—Modeling service standards simulate a condition or activity in a transaction process system by performing a set of equations on a set of data. A model is a mathematical representation of a device or process used for analysis and planning.

Modem (acronym for Modulator-Demodulator)—A device that modulates and demodulates electrical (intelligence) signals. In the computer world, modems are primarily used for converting digital signals into quasi-analog signals for transmission and for reconverting the quasi-analog signals into digital signals. Many additional functions may be added to a modem to provide for customer service and control features.

Modification—A configuration change to an already-produced configuration item.

Modular—Pertaining to the design concept in which interchangeable units are used to create a functional end product.

Modular C4 Packages—A set of capabilities and specific items of equipment matched to meet specific operational needs. Constructed as necessary, modular C4 packages can be interconnected to build C4 systems and networks, based on the range of military operations, C4 assets available, and assigned missions. The baseline C4 modular system initially deployed in response to the range of military operations must be rapidly deployable, robust to enable sufficient C4 in unprepared locations, and provide interoperability and interconnectivity with follow-on forces.

Modulation—In communications-electronics, the encoding of information onto a carrier through the controlled variation of some characteristic of the carrier signal (e.g., frequency, amplitude, and phase modulation or combination thereof). The modulated carrier wave serves to transport the signals within the system or between systems. The modulation process is normally associated with transmitting equipment. Transmission can be by cable/wire or by radio. In the systems associated receiving equipment, demodulation reverses the process and retrieves the original signals or information.

Modulation Transfer Function (MTF)—A parameter using spatial frequency responses to characterize a screen display. The spatial frequency is stated in lines (line pairs) or minimum/maximum intensity pairs per unit distance. The MTF is used as a performance measurement of many optical systems.

Modulator—An electronic device that imposes an intelligence signal on a carrier frequency. In radio communications, the modulator is part of the radio transmitter. Its size can vary from an entire rack of equipment to part of a circuit board, depending on the purpose, size, and radio frequency output power of the associated radio transmitter.

Module—In computing, a segment of core storage.

Monitor—A video display cathode ray tube that displays characters made up of points of light called pixels. It is also called a Computer Screen or Display.

Motion Media—A series of images, viewed in rapid succession, giving the illusion of motion, obtained with a motion picture or video camera.

Moving Pictures Experts Group (MPEG)—A compression method of storing movie files in digital format.

Multi-Beam Antenna (MBA)—An antenna that provides multiple-shaped patterns for selected coverage areas on the earth’s surface.

Multi-Level Precedence and Preemption (MLPP)—The capability to originate calls based on precedence and to preempt calls of lower precedence already established within the network. Defense Switched Network precedence levels are: Priority, Immediate, Flash, and Flash Override.

Multifunction Switch (MFS)—In telecommunications, a Defense Switched Network (DSN) nodal switch which combines the functions of a tandem nodal switch and an end office. There is no physical or electrical division between the tandem and end-office functions. Functional differentiation is accomplished through software tables. This switch interfaces with other DSN switches via interswitch trunks. As a part of the DSN, MFSs are interconnected to and supervised by the DSN system subcontrol system.

Multilevel precedence and preemption (MLPP)—In telecommunications, the capability to originate telephone calls based on precedence and to preempt calls of lower precedence in the network.

Multimedia—Pertaining to the processing and integrated presentation of information in more than one form (e.g., video, voice, music, and data).

Multipath—In radio communications, the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more separate paths. This may result in overall weakening or strengthening of the received signal, depending on the phase relationships of the signals.

Multiple Access—The capability of a communications satellite to function as a portion of a communications link between more than one pair of ground terminals simultaneously. Types of multiple access are: Frequency Division, Code Division, and Time Division.

Multiple Media—Transmission media using more than one type of transmission path (e.g., fiber optics, radio, telephone line, and so forth) to deliver information.

Multiplex (MUX)—The process of combining multiple parallel information streams (voice and/or data channels) into a single communications channel. There are a number of different forms or methods of multiplexing. The most common (and oldest) forms are Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM). In FDM each channel is assigned a separate frequency slot within the broader frequency channel of the communications path. In TDM, each channel is assigned a time slot within a time frame large enough to accommodate all channels.

N-Type Material—In electronics, a semi-conductor material doped with an impurity that provides nuclei with loosely bound electrons. These electrons provide negative charge carriers and are the source of current flow through the semi-conductor device.

Name Server—In computing, the name server provides a means of finding an attribute of an entity given the unique name for any entry within the technology environment. Entities can be physical components (computers, workstations, network nodes), logical components (application modules, data storage locations), or users. The name server will be accessed frequently by clients to find addresses for servers and other objects.

Nano (n)—A prefix used to denote one billionth (109)

Nanosecond—(nsec) One billionth of a second.

Narrowband—In data communications, pertaining to a channel with a bandwidth less than that of a voice-grade channel. It is normally used for communications speeds of less than 300 bits per second.

Narrowband Modem—A modem whose modulated output signal has an essential frequency spectrum that is limited to that which can be wholly contained within, and faithfully transmitted through, a voice channel with a nominal 4 kilohertz bandwidth.

Narrowband Signal—In telecommunications, any analog or analog representation of a digital signal whose essential spectral content is limited to that which can be contained within a voice channel of nominal 4 kilohertz bandwidth.

National Communications System (NCS)—The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability.

National Information Infrastructure (NII)—The nationwide interconnection of communications networks, computers, data bases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of communications and information equipment, systems, and networks, including the personnel who make decisions and handle the transmitted information. The NII is similar in nature and purpose to the Global Information Infrastructure but relates in scope only to a national information environment, which includes all government and civilian information infrastructures.

National Institute for Standards and Technology (NIST)—Formerly National Bureau of Standards. The division of the U.S. Department of Commerce that ensures standardization within government agencies. NIST is responsible for the Applications Portability Profile, a set of standards and guidelines for U.S. Government procurement.

National Security Systems—Those telecommunications and information systems operated by the U.S. Government, its contractors or agents, that contain classified information or that involve intelligence activities, involve cryptologic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapon system, or involve equipment that is critical to the fulfillment of military or intelligence missions.

Neper (Np)—In communications-electronics, a standard unit used to express the ratio of two values of amplitude. Like the decibel (dB), it is a dimensionless unit. It is a logarithmic unit based on natural logarithms instead of common logarithms. Where the decibel is commonly used in the United States, the Neper is commonly used in Europe. One Np equals 8.686 dB.

Net Gain/Loss—The overall gain or loss of a transmission circuit.

Network—1. An organization of stations capable of intercommunication but not necessarily on the same channel. 2. Two or more interrelated communications circuits. 3. A system of software and hardware connected to support the exchange of data. 4. A combination of circuits and terminals serviced by a single switching or processing center. 5. Two or more systems connected by a communications medium.

Network Layer—In data communications, a layer in the International Standards Organization's open systems interconnection.

Network Management—The ability to provide fault management, configuration management, security management, accountancy management, and performance management for the network.

Network Protocols—The standardized agreements and their hardware or software implementations used to control the orderly exchange of information on a network and associated data links.

Network Topology—The specific physical or logical arrangement of the elements of a network.

Nodal Switch—A tandem switch in the DSN that connects multiple end offices, provide access to a variety of transmission media, route calls to other nodal switches, and provide network features such as multilevel precedence and preemption. There are two types of nodal switches in the DSN, stand-alone and multifunction switches.

Node—1. A location in a mobility system where a movement requirement is originated, processed for onward movement, or terminated. In network topology, a terminal of any branch of a network or a terminal. 2. A point in a network, either at the end of a communications line (end node) or where two lines meet (intermediate node). 3. In switched communications, a node is the switching point that may also include patching and control facilities. 4. In a data network it is the location of a data station that interconnects data transmission lines. 5. A point in a standing or stationary electromagnetic wave at which the amplitude is minimum.

Noise—In telecommunications, (1) An undesired disturbance within the useful frequency band; the summation of unwanted or disturbing energy introduced into a communications system from man-made and natural sources. (2) A disturbance that affects a signal and that may distort the information carried by the signal. There are many and varied types of noise in a telecommunications system.

Noise Level—In telecommunications, the volume of noise power on a circuit or channel, measured in decibels, usually referenced to a base (such as milliwatt, dBm)

Noise Suppression—1. The reduction of the noise power level in electrical circuits. 2. In radio communications, the process of automatically reducing the (audible) noise in the output of a radio receiver during periods when a carrier is not being received. (Compare: squelch.)

Nomenclature—The combination of an item name and type designation, such as of communications equipment or system, e.g., VHF/UHF Radio Set, AN/TRC-24.

Nominal Bandwidth—The widest band of frequencies, inclusive of guard bands, assigned to a communications channel.

Noncritical Technical Load—That part of the technical (electrical) load of a communications facility not for equipment requiring synchronous operation.

Non-Form Item—A printed product without spaces for entering information. Some non-form items have been entered into the Standard and Optional Form Program so they can be controlled government-wide.

Nonrecord—Information materials that are not part of the legal definition of a record. Includes extra copies of documents kept only for convenience of reference, stocks of publications and of processed documents, and library or museum materials intended solely for reference or exhibition.

Non-repudiation—Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can deny having processed the data.

Non-Return-To-Zero (NRZ) Code—A code having two states termed zero and one, and no neutral or rest condition.

Nonrecurring Pamphlets—Nondirective classified or unclassified publications printed once. They are usually published to inform, motivate, increase knowledge, or improve performance. The term includes leaflets, bulletins, folders, booklets, reports (e.g., special after-action reports, reports with less than 10 percent statistical information), and similar nonrecurring pamphlets. Nonrecurring pamphlets may contain official or unofficial information or both. The term does not include memoranda; authenticated, numbered, administrative pamphlets published under AFI 33-360, Volume 1, *Publications Management Program*, as a part of an activity's or command's official publications system; directives and instructions, regulations, legal opinions and decisions, proceedings, programs for ceremonies, press releases, environmental impact statements and assessments, planning documents, and purely administrative materials, but does include pamphlets produced to complement any of the foregoing types of publications.

Non-Secure (SBU) Internet Protocol (IP) Router Network—A high-speed unclassified data network for DoD that provides interconnectivity among DoD customers and the commercial network.

Nontechnical Load—In a communications installation, that part of the total operational (electrical) load used for general lighting, ventilation, air conditioning, and so forth, required for normal operation.

Nuclear Hardness—1. The measure or extent to which performance of a communications system will degrade in a given nuclear environment. 2. The physical attributes of a system or component that will allow a defined degree of survivability in an environment that includes nuclear radiation and electromagnetic impulse.

Null—In an antenna radiation pattern, a zone in which the effective radiated power is at a minimum relative to the maximum effective radiated power of the main beam.

Null Character—In data communications, a control character that is used as a fill character for transmission or storage. It may be removed from a sequence of characters without affecting its meaning. The null character may, however, have some significance in the control of equipment or formatting.

Null String—In data structures, a string that contains no characters.

Nyquist Sampling Theorem—In digital communications, a theorem that specifies the sampling rate necessary to ensure the original analog signal can be reconstituted from the sampled values. The theorem states the sampling rate must be twice as high as the highest frequency present in the sampled signal.

Object—A passive receiver of information. Access to an object implies access to the information the object contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes. A person, place, thing, concept, event, or activity about which an organization keeps information.

Object Based Language—A programming language that supports some but not all of the characteristics of abstraction, encapsulation, modularity, and hierarchy.

Object Code—Also **Machine Code**. The final result of a language translation; a set of bit patterns interpretable by the electronic circuitry of a computer.

Object Data Base—A data base that holds abstract data types (objects). It can store objects directly from an object-oriented programming language.

Object Link Embedding (OLE)—In computing, a method to transfer and share information between applications. OLE links are similar to direct data exchange (DDE) links, except the source (server) application can be started from within the current (client or receiving) application to edit the linked object. An OLE object can be linked or embedded. A linked OLE object leaves the data stored in the source (server) application file. In an embedded OLE object, the data for the object is stored in the current (client or receiving) application file.

Object Oriented Language—A programming language that fully supports the characteristics of abstraction, encapsulation, modularity, and hierarchy.

Objective Configuration—A configuration that depicts the organization optimum information and resource capabilities needed to support the mission.

Objective Phase—The period, consisting of the years after the midterm phase, in which implementation of the C4I for the Warrior concept will be completed. The technology available during this phase will change the art of conducting warfare significantly.

Obsolete Publication—A rescinded or superseded publication.

Off-Hook—In communications, a condition in which a unit indicates a busy condition to incoming telephone calls.

Off-Line—That condition where devices or subsystems are not connected into, do not form a part of, and are not subject to the same controls as an operational system. These devices may, however, be operated independently.

Offensive Counterinformation (OCI)—Offensive information warfare activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems.

Offensive Information Operations (OIO)—The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction.

Office Automation—In office systems, the use of any form of machine or system that either replaces or simplifies human activities and operations in office environments.

Office Forms—Forms for use only within the originating directorate, division, branch, or section. Major command and field operating agency Information Managers may delegate the control of office forms to the office of primary responsibility. Office forms do not have to be prescribed, and indexing them is optional.

Office of Primary Responsibility (OPR)—Any organizational activity having primary functional interest in, and responsibility for a specific action, project, plan, or program.

Official Mail—Any item processed through the United States Postal Service that pertains exclusively to the business of the United States Government for which the postage and fees are paid by the United States Government.

Official Record—Recorded information, regardless of media, maintained by an agency to comply with its legal obligations or created as a result of its transactions of public business. Excluded as records are library and museum materials, extra copies of documents preserved for convenience or references, stocks of publications, and blank forms.

Omni-Directional Antenna—An antenna whose radiation pattern is non-directional in azimuth.

On-Hook—In communications, a condition in which the telephone is not in use.

On-Line—That condition where devices or subsystems are connected into and form a part of, and are subject to the same controls as an operational system.

On-Line Processing—Processing where individual transactions are entered into the equipment via a terminal. The data entry is processed and a response is transmitted back to the terminal for user dissemination.

One-Time Forms—Forms that satisfy a one-time requirement, are not reprinted, and are obsolete when no longer needed.

One-Time Request—The customer may obtain an order quantity on a one-time basis without changing their average monthly usage.

Open Circuit—1. In telecommunications, a circuit that contains an infinite (very high) impedance (e.g., the circuit is not connected or terminated properly). 2. A communications circuit that is available for use.

Open Loop—A system in which the input signal or information is not influenced by the output of the system.

Open Network—A network that can communicate with any system component (peripherals, computers, or other networks) implemented to the international standard (without special protocol conversion, such as gateways). Also see Open System.

Open Software Foundation (OSF)—A consortium of computer hardware and software manufacturers whose membership includes over 70 of the computer industry's leading companies.

Open Specification—Public specifications that are maintained by an open, public consensus process to accommodate new technologies over time and that are consistent with international standards.

Open System—1. A system with specified standards that can be readily connected to other systems that comply with the same standards. 2. A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered software (a) to be ported with minimal changes across a wide range of systems, (b) to interoperate with other applications on local and remote systems, and (c) to interact with users in a style that facilitates user portability. 2. An open system supports the interoperability of hardware, software, and communications products developed by different suppliers at different times. Because any type of data can be stored (the rules for processing the data are part of the object), the object data base promises fully integrated data bases that will hold data, text, pictures, and voice, essentially an endless variety of ever-changing formats. It is capable of handling complex queries about objects that would be difficult in relational data base programs.

Open Systems Application Program Interface (API)—A combination of standards-based interfaces specifying a complete interface between an application program and the underlying application platform.

Open Systems Architecture—The framework describing the entities (e.g., components and services) and their interrelationships in an open system. Open system architectures and environments are intended to help achieve portability, interoperability, scalability, and cost-effectiveness of systems.

Open Systems Environment (OSE)—A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles.

Open Systems Interconnection (OSI)—Concept for achieving total interoperability of information systems based on a layered, structured hierarchy of specific technical functions required for information transfer. Implies vendor independence in most circumstances.

Open Systems Interconnection Reference Model (ISO-RM)—In data communications, an ISO-RM is intended to coordinate the development of communications interfaces and protocol standards at all levels of communications. The OSI model defines seven functional layers with standardized interfaces between them. The concept of the layers provides for a considerable degree of independence between the multifarious and complicated operations involved in data communications. At each level the process believes it is communicating with its corresponding layer in the receiving host.

Open Wire—Unshielded wire conductors separately supported above the surface of the earth.

Operating Document—A completed form or other document used to facilitate, accomplish, or provide a description or record of a transaction, function, or event. The information in an operating document may provide data or input for a report, but that is not its primary purpose. Examples of operating documents include application forms, purchase orders, personnel actions, bills of lading, payrolls and time sheets, inspection or audit reports, and reports that involve direct command and control of military forces or cryptological activities related to national security.

Operating System—1. The system that controls a computer's activities, and by which it uses applications programs. 2. An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in operating a computer system. Operating systems may perform input or output, accounting, resource allocation, storage assignment tasks, and other system-related functions.

Operational Architecture—A description of tasks, operational elements, and information flows required to accomplish or support a DoD function or military operation. It contains descriptions of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in sufficient detail to ascertain specific interoperability requirements. Also referred to as functional architecture.

Operational Load—The total electrical power requirements for a communications facility.

Operational Test and Evaluation (OT&E)—Testing and evaluation conducted in as realistic conditions as possible throughout the system's life cycle. Tests are conducted to verify that an information system is installed and capable of performing its operational mission as outlined in program documentation. OT&E is used to verify operating instructions, computer documentation, training programs, publications, and handbooks.

Operations Security—(OPSEC) A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities (1) to identify those actions that can be observed by adversary intelligence systems, (2) determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and (3) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Optical Character Recognition (OCR)—The analysis and translation of a graphic representation of text into a coded form such as American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC). 2. The method of inputting data into a computer by reading printed or hand-written characters.

Optical Crosstalk—Optical crosstalk, or bleeding, occurs when the light from the incorrect video image gets through. When referring to stereoscopic images, the right eye's image is visible to the left eye or vice versa.

Optical Digital Technologies (ODT)—Represent technologies that use the reflective properties of light and an optical recording surface to capture, encode, decode, and store data. ODT predominantly encompass optical media, optical drives, and scanners.

Optical Instrumentation—Use of optical systems, coupled with photographic or television recording devices, that may include audio, to record scientific and engineering phenomena for the purpose of technical measurement and evaluation. It may also include recording data to correlate optical images to time or space positions or other engineering data.

Order Source—In this functional description, an order source is the office the user has an account with.

Orderwire Circuit—A voice or data circuit used by technical control and maintenance personnel to coordinate operations and maintenance actions for the control and restoration of communications circuits and systems.

Oscillator—In electronics, a device that produces a sinusoidal, square wave, or pulsed signal of a specified frequency. These signals are used in radio and communications equipment for a variety of purposes, such as tone or frequency generators, timing and synchronization.

Other Government Agency Forms—Government agencies such as the Department of the Treasury, Office of Personnel Management, and Department of Veterans Affairs develop and approve their agency forms.

Out-Of-Band Signaling—Signaling that utilizes frequencies within the guard band between channels or bits other than information bits in a digital system.

Output—Signals that move information from the computer's internal storage to peripheral devices, such as printers, modems, and disk or tape drives.

Output Product—The final result of the peripheral device, such as a disk, paper copy, or microform created from the output signals.

Outside Plant—That portion of intrabase communications systems extending from the main distribution frame outward to the telephone instrument or the terminal connections for other technical components.

Ovality—In an optical fiber, the degree of deviation from perfect circularity of the cross-section of the core or cladding.

Over-The-Air Updating (OTAU)—C4I for the Warrior OTAU is the push process by which the warrior's pre-planned essential elements of information data bases are automatically updated by elements of the infosphere, which is the combination of information sources, fusion centers, and distribution systems that the warrior requires to pursue his operational objectives. Only value-added information will be sent over the infrastructure. These updates are defined by information path rules, or info triggers that describe what, when, and how often the updates occur.

Overhead Bit—A bit other than an information bit. Included for control or error-checking purposes.

Overmodulation—The condition that prevails when the instantaneous level of the modulating signal exceeds the value necessary to produce 100 percent modulation of the carrier.

Overprinting—The printing of pertinent identical entries (e.g., agency name, accounting codes, etc.) in a caption area on a form. Overprints are not exceptions.

Overtones—In communications-electronics, frequencies that are multiples of the fundamental frequency.

Packet—A group of binary digits including data and control elements that is switched and transmitted as a composite whole. The data and control elements, and possibly error control information, are arranged in a specified format.

Packet Internet Groper (PING)—In Transmission Control Protocol/Internet Protocol, a protocol function that tests the ability of a computer to communicate with a remote computer by sending a query and receiving a confirmation response.

Packet Switching—A data transmission process, utilizing addressed packets, where a channel is occupied only for the duration of transmission of the packet. A method of message transmission in which each completed message is assembled into one or more packets that can be sent through the network, collected and re-assembled into the original message at the destination. The individual packets need not be sent by the same route.

Paired Cable—A cable made up of one or more separately insulated pairs or lines, none of which are arranged with others to form quads. See also Quadded Cable.

Parabolic Antenna—An antenna consisting of a parabolic reflector and a radiating or receiving element at or near its focus. If the reflector is in the shape of a paraboloid of revolution, it is called a Paraboloidal

Reflector. Cylindrical paraboloids and partial paraboloids are also used.

Parallel Port—A port through which two or more data bits are passed simultaneously, such as all the bits of an 8-bit byte, and that requires as many input channels as the number of bits that are to be handled simultaneously.

Parallel Transmission—In data communications, the simultaneous transmission of signal elements constituting the same code (e.g., each bit of a word is sent simultaneously on an individual wire). It has a higher bit rate then corresponding serial transmission, but requires eight wires to convey individual bytes and is therefore mainly used for transmission over short distances.

Parameter—Quantity or constant whose value varies with the circumstances of the application.

Parametric Amplifier—A radio frequency amplifier that has a very low noise level and is especially designed to amplify very weak signals. In radio communications, the parametric amplifier is used in the receivers of satellite earth terminals and wideband radio communications systems.

Parity—In binary-coded systems, a condition obtained with a self-checking code such that in any permissible code expression the total number of ones or zeroes is always even or odd.

Parity Bit—A check bit appended to an array of binary digits to make the sum of all the binary digits, including the check bit, always odd or even.

Parity Check—A check that tests whether the number of ones (or zeroes) in an array of binary digits is odd or even. Odd parity is standard for synchronous transmission and even parity for asynchronous transmission.

Passband—In communications, the range of signal frequencies that can be satisfactorily transmitted on a given channel (e.g., the passband on voice-grade channels is 300-3400 hertz).

Passive Device—A device that does not require a source of energy for its operation. Examples of passive devices are resistors, capacitors, diodes, filters, and so forth.

Passive Reflector/Repeater—In radio communications systems, a device used to route a line-of-sight microwave radio beam over or around an obstruction. For example, two parabolic antennas connected back-to-back, or an arrangement of one or two flat reflectors used as a mirror. The device requires no electrical power to operate, hence the term passive.

Password—1. A secret word or distinctive sound used to reply to a challenge. 2. A protected word or string of characters that identifies or authenticates a user for access to a specific system, data set, file, record, and so forth.

Patch—In telecommunications, to connect circuits together, usually temporarily, by means of a cord (cable) known as a patch cord. 2. In computer programming, (a) to replace a small set of instructions with a modified or corrected set; and (b) to modify a program by changing its object code rather than its source code.

Patch and Test Facility—An organic element of a communications station or terminal facility that functions as a supporting activity, under the technical supervision of a designated technical control facility.

Patch Bay—An assembly of hardware so arranged that a number of circuits, usually of the same or similar type, appear on jacks for monitoring, interconnecting, and testing purposes. Patch bays are used in technical control facilities, patch and test facilities, and telephone exchanges.

Patch Panel—One segment of a Patch Bay.

Path Loss—The decrease in power in transmission from one point to another along a propagation path. In radio communications systems, it is taken as the loss in power of the radio signal between the transmitter and receiver antennas, expressed in decibels.

Path Profile—A graphic representation of the physical features of a propagation path in the vertical plane, containing both end points of the path, showing the surface of the Earth as well as buildings, trees, and other obstacles that may obstruct the radio signal.

Peak Envelope Power (of a radio transmitter)—The average power supplied to the antenna transmission line by a transmitter during one radio frequency cycle at the crest of the modulation envelope taken under normal operating conditions.

Perigee—In satellite communications, the point at which a satellite is at a minimum distance from Earth in its orbit. Compare Apogee.

Periodic Antenna—An antenna that has an approximately constant input impedance over a narrow range of frequencies. Synonym: Resonant Antenna.

Periodical—Any classified or unclassified Air Force magazine or newsletter publication (with a consistent format, content, and purpose) published at least once a year to provide information pertinent to the publishing activity. Its purpose is to disseminate information and material necessary to the issuing activity. Periodicals may refer to or quote directive information, but are not directive publications.

Peripheral—In computing, (a) a device, under control of the central processing unit, that performs an auxiliary action in the system (e.g., input/output, backing storage) and (b) any equipment that provides the computer with additional capabilities distinct from the central processing unit. Examples are a printer, mouse, disk drive, and so forth.

Peripheral Equipment—In data processing, any equipment distinct from the central processing unit that may provide the system with additional capabilities.

Peripheral Interface Adapter (PIA)—In computing, a device that provides interface functions between the computer bus and its peripherals.

Permanent Records—Records the Archivist of the United States has appraised and approved for permanent retention by the United States Government, and for accessioning into the National Archives.

Personal Computer (PC)—A computer system capable of stand-alone operation and designed for use as a single workstation. Consists of a keyboard, monitor, central processing unit, printer, and disk drive.

Personal Computer Memory Card International Association (PCMCIA)—A standard for the form and interconnection method for credit card size enclosed circuit boards that add various peripherals and memory storage, particularly for laptop computers and personal digital assistants.

Personal Digital Assistant (PDA)—A hand-held computer, usually with a pen-based user interface and wireless communication capability for fax, data, and paging.

Personal Identifier—A name, number or symbol that is unique to an individual, usually the person’s name or Social Security number.

Personal Information—Information about an individual other than items of public record.

Personal Mail—Any item processed through the United States Postal Service addressed to or from an individual that does not pertain to the official business of the United States Government.

Peta- (P)—A prefix denoting 1000 trillion (1015). (This quantity is increasingly used within the imagery community).

Phase Hit—In a communications channel or circuit, a momentary disturbance caused by sudden phase changes in the signal.

Phase Jitter—Rapid, repeated phase disturbances that result in the intermittent shortening or lengthening of signal elements.

Phase Locked Loop (PLL)—In communications-electronics, an electronic circuit that serves as a frequency control or stabilizing device; it controls a frequency generator (oscillator) so that it maintains a constant phase angle relative to a reference signal.

Phase Modulation—In radio communications, a method of modulation in which the phase of the sinusoidal carrier is varied in accordance with the modulating signal. Compare frequency modulation.

Phase Shift—The change in phase of a periodic signal with a reference.

Phase Shift Keying (PSK)—In data communications, a method of changing the phase of the sinusoidal signal to represent binary data. If only two discrete phases are employed, each phase corresponds to a binary 1 or 0; if four phase shifts are used each one may correspond to a dibit.

Phased Array—An arrangement of antennas (of any type) in which the signal feeding each antenna is varied in such a way that radiation is reinforced in a desired direction and suppressed in undesired directions. Rapid scanning in azimuth or elevation can be accomplished with such arrays.

Psychological Operations (PSYOP)—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or influence foreign attitudes and behavior favorable to the originator's objectives.

Pica—A printer's unit of measure used principally in typesetting. One pica equals approximately one-sixth of an inch. It is used for linear measurements of type. (A pica gauge is the printer's measuring tool.) There are 12 points to 1 pica, or 6 picas to 1 inch. The length of the line is specified in picas, as well as the depth of a type area. Inches are never used in type measurement.

Pico (p)—A prefix used to denote one trillionth (1012).

Picowatt—(pW) A unit of electrical power equal to one trillionth of a watt.

Piezoelectric—Electric polarity due to pressure especially in a crystalline structure.

Pilot (frequency)—In telecommunications, a signal, usually a single frequency, transmitted over a system for supervisory, control, synchronization, or reference purposes.

Pitch—The number of characters in 1 inch along a typed line. This measure does not apply to proportional spacing. Also, pitch is sometimes used as another term for character spacing.

Pixel—1. Physical picture elements. 2. Contraction for picture element. A pixel is a single dot on a display screen.

Planar Array—An antenna in which all of the elements, both active and passive, are in one plane.

Plant—All the facilities and equipment used to provide telecommunications services.

Platemaker—Equipment printers used to make a master imaging plate for offset printing. The equipment operates by an electrostatic, direct photographic process or by an intermediate (negatives or positives) process.

Plesiochronous—In time division multiplexing, the relationship between two signals such that their corresponding significant instants occur at nominally the same rate, any variations being constrained within a specific limit.

Point Of Presence (POP)—An installation of telecommunications equipment, usually digital leased lines and multi-protocol routers.

Points—A printer's unit of measure used principally in typesetting. Type size is measured in points. Line length measure is in picas and points. The point measures .0138 or approximately 1/72nd of an inch. In other words, there are 72 points to the inch. All type is designated in points.

Polar Orbit—An orbit for which the angle of inclination is 90 degrees. A satellite in polar orbit will pass over both the north and south geographic poles once per orbit.

Polarization—That property of a radiated electromagnetic wave describing the time varying direction and amplitude of the electric field vector. The position of an antenna is described according to the polarization of the electric field (of the radio wave) emitted from, or received by, the active element of the antenna. For example, in a horizontally polarized antenna, the active element is horizontal to the surface of the Earth.

Policy—A statement of important, corporate level direction that guides Air Force decisions. Policy is enforceable, and compliance with policy is measurable. Policy is the framework connecting the abstract ideas or principles contained in vision, mission, and purpose statements to the specific and concrete statements of plans, goals, and objectives. Policy can be viewed as establishing bounds within which the organization will operate. Policy provides both a focus for Air Force action and a guide for the behavior of the organization and its members.

Pop-Up Menu—A list of options that appear on the display screen as a window.

Portability—The ease with which software can be transferred from one information system to another.

Portable Operating System Interface for Computer Environments—(POSIX) 1. The term POSIX has been evolving into a term with a number of different meanings. POSIX is sometimes used to denote the formal standard ISO/IEC 9945-1, sometimes to denote that standard plus related standards and drafts emerging from IEEE P1003.x working groups, and sometimes to denote the groups themselves. Reference is preferred to the original POSIX standard by its standard designation ISO/IEC 9945-1 and not by the term POSIX. 2. A collection of evolving standards intended to provide a common interface and functionality for applications to access operating system services.

Porting—The process by which a software application is made operational on a computer architecture different from the one on which it was originally created.

Positive Feedback—In communications-electronics, a signal feedback arrangement in which part or all of the output signal of a device, usually an amplifier, is effectively added to the input signal or fed back into the input circuit for gain control or circuit stabilization purposes. Under certain conditions this can result in self-sustained oscillations.

Postalize—In telecommunications, to structure rates or prices so that they are not distance sensitive, but depend on other factors, such as call duration, time of service, and time of day.

Post Office Protocol (POP)—A protocol designed to allow single users to read mail from a server. There are three versions: POP, POP2, and POP3. The POP is used to transmit the stored mail from the server to the user's local mailbox on the user's client machine.

Posting—Adding or removing pages, or writing in changes or items from a supplement to a basic publication.

Power Absorbing Device (PAD)—A network of electronic components designed to attenuate audio or radio frequency signals by a fixed amount with a minimum of distortion.

Precedence—In telecommunications, a ranking assigned to indicate the degree of preference to be given in the processing and protecting of a telephone call. Originators of a precedence call may elect to use their highest authorized precedence or any lesser precedence. Precedence levels (from lowest to highest) are: Routine, Priority, Immediate, Flash, and Flash Override.

Predictive Modeling—Use of a model to predict the actual response of a system or process.

Prescribed Form—A form prescribed in a DoD publication. The Office of the Assistant Secretary of Defense approves and mandates their use by the military departments. A standard or specialized Air Force publication prescribes them, except when prescribed in DoD issuances.

Preservation—1. The provision of adequate facilities to protect, care for, or maintain records. 2. Specific measures, individual and collective, undertaken to maintain, repair, restore, or protect records.

Pretty Good Privacy (PGP)—A software encryption capability distributed on the internet for assuring the privacy of user E-mail messages. PGP uses public key encryption. **NOTE:** All encryption capabilities used by the Air Force must be validated by NIST or, endorsed by NSA, depending on the type of information to be protected prior to use.

Prime Word—A word used in a data element name that represents the data grouping to which the data element belongs.

Printer—Any output device, including laser beam, dot-matrix, letter-quality, or line printer, that converts computer codes to printed characters on paper.

Printing—Any process that produces multiple copies of printed material. This includes composition, platemaking, press work (includes electronic printing), binding, and microform production. It does not include office photocopying or any other method that is capable of only limited production. Unless designated as a printing plant or duplicating facility, the normal output (6 copies or less) of data processing installation is considered limited production. There are two kinds of Air Force printing: (a) departmental printing which is required throughout the Air Force, and (b) field printing which is done by a major command, field operating agency, or direct reporting unit mainly for its own use.

Prior Master File—A file that was at one time the current master file, but the master file updating process superseded it. Usually second, third, or fourth generation tapes (or other media) reflecting superseded data or a superseded master file that has lost all or some of its data.

Privacy Act Request—An oral or written request by an individual about his or her records in a system of records.

Private Branch Exchange (PBX)—A subscriber-owned telecommunications exchange that usually includes access to the public switched network.

Private Key—A cryptographic key used in the dual key system, uniquely associated with an entity, and not made public; it is used to generate a digital signature. This key is linked mathematically with a corresponding public key.

Procedural Interface Standards—Specifications for exchanging information across an interface. The standards define format, language, syntax, vocabulary, and interface operating procedures. Information exchanged among C4 systems using a tactical digital information link, modulation transfer function, and other combat data links.

Processor—In a computer, a functional unit that interprets and executes instructions.

Profile—A set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards necessary for accomplishing a particular function.

Program—In computing, a sequence of instructions used by a computer to perform a particular function or solve a given problem.

Programmable Read-Only Memory (PROM)—In computing, a storage device that, after being written to once, becomes a read-only memory.

Programming Language—An artificial language that is used to generate or express computer programs.

Project Support Agreement (PSA)—A document prepared by the C4 systems program engineer that describes: what equipment to install; sites agreed on; supporting construction; services required; operational, technical, or other constraints affecting a C4 systems requirement; and responsibilities of the host base civil engineer, base C4 systems staff, and other supporting activities.

Prompt—Text or graphic display that indicates the start point for user-generated actions. This term is also used for software-generated instructions for process confirmation.

Propagation—In radio communications, the motion of electromagnetic waves through or along a medium or in a vacuum.

Protection Interval (PI)—In high-frequency radio automatic link establishment, the period between changes in the time-of-day portion of the time-varying randomization data used for encrypting transmissions.

Protocol—In data communications, (1) a set of rules governing network functionality (the open system interconnection reference model uses sets of communication protocols to facilitate communications between computer networks and their components), and (2) a formally specified set of conventions governing the format and control of inputs and outputs between two communicating systems.

Protocol (Software)—A formal set of conventions or rules that govern the interactions of processes or applications within a computer system or network. Also, a set of rules that govern the operation of functional units to achieve communication.

Pseudorandom Noise—Noise that satisfies one or more of the standard tests for statistical randomness. Although it seems to lack any definite pattern, there is a sequence of pulses that repeat after a very long time interval.

Psophometer—In communications, a noise measuring set; an instrument that measures circuit noise voltages. The psophometer is calibrated with a tone of 800 Hz, 0 dBm, instead of the more commonly used test tone of 1 kHz.

Public Burden or Burden Hours—The total time, effort, or financial resources required to respond to a collection of information, including the time it takes to read or hear instructions; to develop, modify, construct, or assemble any materials or equipment; to conduct tests, inspections, polls, observations, or the like necessary to obtain the information; to organize the information into the requested format; to review its accuracy and the appropriateness of its manner of presentation; and to maintain, disclose, or report the information.

Public Domain Software—Software released to the general public for use without payment or restriction. Generally, no support or software accuracy is promised.

Public Key—A cryptographic key used in the dual key system, uniquely associated with an entity, and not made public; it is used to generate a digital signature. This key is linked mathematically with a corresponding private key.

Public Key Infrastructure—In data communications, the methodology that allows business to be conducted electronically with the confidence that (1) the person sending the transaction is actually the originator, (2) the person receiving the transaction is the intended recipient, and (3) data integrity has been maintained.

Public Protection Clause—Regardless of any other provision of law, no person can be penalized for failure to comply with any collection of information that does not display a currently valid Office of Management and Budget (OMB) control number; or, in the case of information required by law or to obtain a benefit that is submitted to nine or fewer persons, fail to state that it is not subject to OMB review under The Act. If an agency has imposed a collection of information as a means to satisfy or prove a condition for receiving a benefit, or to prevent a penalty, and the information collection does not display a currently valid OMB control number, the agency won't treat a person's failure to comply as grounds for withholding the benefit or imposing the penalty. The agency shall instead permit respondents to prove or satisfy the legal conditions in any other reasonable manner.

Publishing Bulletin (PB)—Provides Publishing Distribution Office System users at all levels with information on the current status of publications and forms. PBs are issued by the AFPC, CPDCs, NAF, PDO, and so forth.

Pull-Down Menu—List of options attached to a selection on a menu bar which are tailored to the needs of each program.

Pulse Amplitude Modulation (PAM)—That form of modulation in which the amplitude of the pulse carrier is varied in accordance with some characteristics of the modulating signal.

Pulse Code Modulation (PCM)—In telecommunications, that form of modulation in which the modulating signal is sampled, the sample quantized and coded, so that each element of information consists of different kinds of numbers of pulses and spaces.

Pulse Duration Modulation (PDM)—In telecommunications, that form of modulation in which the duration of a pulse is varied in accordance with some characteristic of the modulating signal.

Pulse Position Modulation (PPM)—In telecommunications, that form of modulation in which the positions in time of the pulses are varied in accordance with some characteristic of the modulating signal without modifying the pulse width.

Quadbit—In data communications, four bits that are transmitted in a single baud.

Quadded Cable—A cable formed by taking four, or multiples of four, paired and separately insulated wires and twisting these together within an overall jacket.

Quadrature—1. The state of being separated in phase by 90 degrees. 2. Pertaining to the phase relationship between two periodic quantities varying with the same period (i.e., the same frequency or repetition rate), when the phase difference between them is one-quarter of their period.

Quadrature Amplitude Modulation (QAM)—In data communications, a method of converting digital signals into analog signals for transmission over a telephone network. It combines both amplitude and phase modulation techniques.

Quadruple Diversity—In radio communications, the term applied to the simultaneous combining of, or selection from, four independently fading radio signals and their detection through the use of space, frequency, angle, time, or polarization characteristics or combinations thereof.

Qualitative Data—A data value that is a non-numeric description of a person, place, thing, event, activity, or concept.

Quantitative Data—A numerical expression that uses Arabic numbers upon which mathematical operations can be performed.

Quantization—In time division multiplexing, a process in which the continuous range of values of a signal is divided into non-overlapping, but not necessarily equal subranges, and to each subrange a discrete value of the output is uniquely assigned. Whenever the signal value falls within a given subrange, the output has the corresponding discrete value.

Quantizing Noise—In time division multiplexing, an undesirable random signal caused by the error of approximation in a quantizing process and which manifests itself as a background noise on a telecommunications channel. It is solely dependent on the particular quantization process used and the statistical characteristics of the quantized signal.

Quasi-Analog Signal—A digital signal that has been converted to a form suitable for transmission over a specified analog channel.

Quick-Fix Phase—One of several phases of the C4I for the Warrior concept. The quick-fix phase includes the six years of the program objective memorandum development and acquisition cycle. This phase is used to resolve current critical C4I interoperability problems.

Rack—Pertaining to the metal or other type of vertical frame or chassis on which panels of electrical or electronic equipment may be mounted, usually 19 inches wide.

Radiating Element—Also referred to as the Active Element. In radio communications, the element of a transmitting antenna or antenna system from which the electromagnetic energy is radiated.

Radiation—In radio communications, the emission of energy as electromagnetic waves.

Radiation Hazards (RADHAZ)—In communications, electromagnetic radiation hazards and concerns about the effects on the human body of non-ionizing radiation caused by exposure to high-power transmitters or electronic equipment that produces x-rays.

Radiation Pattern—The variation of the field intensity of electromagnetic energy radiated from an antenna as a function of direction. The radiation pattern of an antenna for a given frequency or range of frequencies is the same whether transmitting or receiving.

Radio—A general term applied to the use of radio waves as a method of communicating over a distance by modulating electronic signals and radiating these signals as electromagnetic waves.

Radio Channel—An assigned band of frequencies sufficient for radio communications. Used in conjunction with a predetermined letter, number, or code word to reference a specific radio frequency.

Radio Day (RAYDAY)—A telecommunications term used to represent message creation and station log entry dates. RAYDAYS are numbered sequentially from the first day of January (001 for 1 January, 002 for 2 January, etc.). Each RAYDAY begins at 0000 Greenwich mean time.

Radio Frequency (RF)—In radio communications, any frequency that can be used for communications by means of electromagnetic radiation.

Radio Frequency Bandwidth—The difference between the highest and lowest emission frequencies in the region of the carrier or principal carrier frequency.

Radio Frequency Interference (RFI)—A manmade or natural, intentional or unintentional, electromagnetic propagation that results in unintentional and undesirable responses from, or performance degradation or malfunction of, electronic equipment.

Radio Frequency Spectrum—Includes the frequencies from 3.0 kilohertz (kHz) to 400 gigahertz (GHz). The wavelengths associated with those frequencies range from 100 kilometers to 0.1 millimeter, respectively. The presently allocated radio frequency spectrum is from 9 kHz to 381 GHz.

Radio Horizon—The locus of the points at which direct waves from an antenna become tangential to the Earth's surface. Near the surface of the Earth, the radio horizon generally extends beyond the Earth horizon due to atmospheric and other influences on the radio waves.

Radio Relay—The transmission and reception of radio signals between stations of a terrestrial point-to-point radio communications system. Radio relay links may form part of the connection between a satellite earth station and switching centers.

Radio Repeater (Station)—In radio communications, a station in a radio relay system whose equipment is in a special back-to-back configuration that retransmits all communications entering its receivers.

Radio Teletypewriter (RTTY)—A teletypewriter employed in a communications system using radio circuits. Also referred to as "radio teletype systems."

Radio Wave—An electromagnetic wave of a frequency arbitrarily lower than 3000 gigahertz. Synonym: **Hertzian Wave**.

Random Access Memory (RAM)—Computer memory that stores and recalls information in any order or sequence. This type of memory is used for temporary storage. RAM requires electrical power to remember information; all information in RAM is lost when the electrical power to the unit is turned off.

Random Noise—In telecommunications, system or circuit noise consisting of a large number of random transient disturbances that is unpredictable except by statistical means.

Randomizer—An electronic device used to invert the sense of pseudorandomly selected bits of a bit stream to avoid long sequences of bits of the same sense.

Read-Only Memory (ROM)—A computer memory that stores permanent information. This information is constant and cannot be erased or changed, even when the electrical power to the unit is turned off. All personal computers contain programs in ROM that execute when the computer is turned on.

Reader—A device capable of sensing information stored in an off-line memory medium (e.g., paper, cards, tape, and so forth) and generating equivalent information in an on-memory device.

Real Time—Pertaining to the timeliness of data or information that has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays.

Real-Time Processing—A form of processing that controls an environment by receiving data, processing it, and taking action to return results in time to affect the functioning of the environment at that time.

Received Signal Level (RSL)—The value of a specified bandwidth of signals at the receiver radio frequency input terminals relative to an established reference.

Recipient Agency—An agency or contractor that receives the records and actually performs the computer match.

Recognition Memory (REM)—In character recognition, a read-only memory in the optical character reader holding the bit patterns of characters in the font. This data is pattern matched with the corresponding information from the input character.

Record—Any information about an individual.

Record Copy—The official or file document that you so mark and recognize, complete with enclosures or related papers.

Records—All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.

Rectangular Waveguide—In radio communications, a waveguide of rectangular cross-section used for the transmission of radio frequency signals over relatively short distances (e.g., between the transmitter or receiver and the antenna).

RED Switch—A voice telephone switching system designed and installed to allow for processing RED (unencrypted) secure conversations. The system has adequate isolation between channels to prevent crosstalk. The distribution system provides adequate shielding ensuring radiation of RED data does not occur. The design allows no multiple-party access without the knowledge of the principal users. Subscribers are placed in and out of service when station equipment is not under the scrutiny of properly cleared persons. RED Switch interfaces provide encryption and allow subscribers access to other secure networks.

RED/BLACK Concept—The concept where the electrical and electronic circuits, components, equipment, and systems, which handle plain language information in electric signal form (RED) are separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between such circuits, components, equipment, and systems, and the areas in which they are located.

Reference Circuit—A hypothetical circuit of specified length and configuration with defined transmission characteristics primarily used as a reference for the performance of other circuits and as a guide for planning and engineering circuits and networks.

Reference Frequency—A frequency having a fixed and specific position with respect to the assigned frequency. The displacement of this frequency with respect to the assigned frequency has the same absolute value and sign that the displacement of the characteristic frequency has with respect to the center of the frequency band occupied by the emission. Also see Characteristic Frequency.

Reflective Array Antenna—An antenna system, such as a billboard antenna, in which the driven elements are situated at a predetermined distance from a surface designed to reflect the signal in a desired direction.

Reflector—In radio communications, one or more conductors or conducting surfaces for reflecting radiant energy, such as part of an antenna system.

Refraction—The bending of a sound, radio, or lightwave as it passes obliquely from one medium to another medium in which its speed is different.

Regency Net—A high frequency radio network that combines the former Cemetery and Inform networks. Regency Net consists of both mobile and fixed stations.

Regenerative Feedback—In an electronic device or circuit, feedback in which the portion of the output signal that is returned to the input of the device has a component that is in phase with the input signal.

Regenerative Repeater—An electronic device in which the received pulse signals are amplified, reshaped, retimed, and transmitted to the next destination. Synonym: Regenerator.

Register—A memory device, usually high speed, for the temporary storage of one or more words to facilitate arithmetical, logical, or transferal operations.

Registration Authority—A person or organization having authority over a portion of the directory information tree.

Reliability—The probability that an item (C4 system, equipment, assembly, or component) will perform its intended function for a specified interval under stated conditions. The overall reliability of a system is measured in terms of the mean time between failure, and mean time to repair.

Remote Data Base Access (RDA)—The interconnecting of data base applications among heterogeneous environments by providing standard open system interconnection application protocols to establish a remote connection between data base client and data base server.

Remote Switching Terminal—An electronic remote switch placed at a subordinate wire center for subscriber lines and normally considered a part of the main switching equipment. A concentrator installed at a remote location to reduce the number of trunks needed to connect remote subscribers to the main switching equipment may serve the same purpose. It may rely on the main telephone system for processor control supervision, trunking, and operator assistance.

Remote Switching Unit (RSU)—A part of an electronic switch located separate from the main switch. It receives its commands from the parent switch but is capable of connecting local users to each other without the need to route them through the parent switch. This limits the number of connections between the local area and the parent switch.

Reorder Point—The point at which a stock replenishment requisition would be submitted to maintain the predetermined or calculated stock objective.

Repair Parts—Consumable bits and pieces; that is, individual parts or nonreparable assemblies, required for the repair of spare parts of major end items.

Report Control Symbol (RCS)—A standard agency designation (control number) for a report consisting of letters or numbers indicating that the report has been reviewed and approved according to DoD and Air Force-directed procedures.

Reprographics—Duplicating, copying, micrographics, and related processes.

Repudiation—The denial by a message originator or recipient that a message was sent or received. In the Defense Message System, the message signature ensures that an originator cannot repudiate the message.

Requirement—A need for a new or improved (information processing) capability which when satisfied will result in an increase in the probability of operational mission success or a decrease in the cost of mission support.

Requirement (Publications)—A formal request that a subaccount representative submits to the customer account representative (CAR), to establish a continuing need for a publication and all of its changes and revisions. The CAR consolidates these requirements and submits them to the publishing distribution office (PDO). The PDO consolidates requirements from all CARs and submits them to the Air Force Publishing Distribution Center or the major command, field operating agency, or the direct reporting unit's publishing distribution center.

Requirements Process—A three-step process that identifies C4 systems requirements, develops a certified technical solution, and allocates resources.

Requisition (Publications/Forms)—A demand or request for publications or forms. Unlike a requirement, a requisition is an order for the actual material. Often requisitions and requirements are submitted at the same time for a publication. Forms are only requisitioned and may never be put on requirement.

Retail Customers—A customer that purchases a publication. Retail customers cannot be put on requirement for a publication.

Retention Period—The length of time the Air Force keeps a record before disposing of it according to the disposition schedules. Records not authorized for a specified disposition have a retention period of permanent.

Retrograde Orbit—Of a satellite orbiting the Earth, an orbit in which the projection of the satellite's position of the (Earth's) equatorial plane revolved in the direction opposite that of the rotation of the Earth.

Return Loss—The ratio, at the junction of a transmission line and a terminating impedance, of the reflected wave to the incident wave, expressed in decibels. More broadly, Return Loss is the loss in power experienced by an electrical signal and is a measure of the dissimilarity between two impedances.

Return-to-Zero (RZ) Code—A code form having two information states called zero and one, and having a third state or condition to which each signal returns during each period. See also Non-Return-to-Zero Code.

Reverse Engineering—The inference and documentation, to a specified level of detail and business generalization, of models of data and information structures, and business rules underlying one or more current or proposed data processing systems.

Rhombic Antenna—A long-wire antenna used in high frequency radio communications and noted for its high efficiency. The antenna is composed of long-wire radiators comprising the side of a rhombus, hence its name. Its disadvantage is the relatively large ground area required because of its size.

Ribbon Cable—1. Any cable constructed as a ribbon with parallel elements. 2. A fiber optic cable in which the optical fibers are held in grooves and laminated within a flat semi-rigid strip of material, such as plastic, that positions, holds, and protects them.

Ring Latency—In a computer ring network, such as a token ring, the time required for a signal to propagate once around the ring.

Round Trip—In satellite communications, the distance from a transmitting ground station through the satellite to a receiving ground station and return via the satellite to the originating station. This distance is used to compute round trip delay time.

Route—1. In communications system operations, the geographical path of a circuit in establishing a chain of connections. 2. To construct the path a circuit is to take in a communications network going from one station to another or from source to destination.

Router—In data communications, a device used to interconnect two or more networks. Routers operate at the network layer (layer 3) of the open system interconnection reference model.

Routine Use—A disclosure of records to individuals or agencies outside DoD for a use that is compatible with the purpose for which the Air Force created the records.

Rubidium Clock—A clock containing a quartz oscillator stabilized by a rubidium standard.

Rubidium Standard—A frequency standard in which a specified hyperfine transition of electrons in rubidium-87 atoms is used to control the output frequency. A rubidium standard consists of a gas cell through which an optical signal is passed. The gas cell has inherent inaccuracies that relegate the rubidium standard to its status as a secondary standard.

S-Band—In radio communications, the frequency range of 2-4 gigahertz. **NOTE:** Letter designators of radio frequency bands are imprecise and legally obsolete.

Safeguard (Storage Safeguard)—These forms are not releasable outside the DoD since they could be put to unauthorized or defaudulent use.

Satellite—An object or vehicle orbiting, or intended to orbit, the Earth, moon, or other celestial body.

Satellite Access—In satellite communications, the establishment of contact with a communications satellite space station.

Satellite Communications Control Plan—A master plan that provides information for the operational benefit of all users of a particular space segment, and which describes the control exercised by a master communications station to ensure that all units of the associated earth segment operate within their assigned parameters and according to prescribed procedures.

Satellite Earth Terminal—A ground communications facility, part of a satellite communications link, that processes, transmits, and receives communications signals between the Earth and the satellite.

Satellite Link—In satellite communications, a radio link between a transmitting Earth station and a receiving Earth station through one satellite. A satellite link comprises one uplink and one downlink.

Saturation—In a communications system, the condition in which a component of the system has reached its maximum traffic handling capacity.

Scalability—1. The ability to use the same application software on many different classes of hardware/

software platforms from personal computers to supercomputers (extends the portability concept). The capability to grow to accommodate increased workloads. 2. The ease with which software can be transformed from one graduated series of application platforms to another.

Scatter—The process where the direction, frequency, or polarization of electromagnetic (radio) waves are changed when the waves encounter one or more discontinuities in the medium that have lengths on the order of a wavelength. See: Ionospheric Scatter and Tropospheric Scatter.

Scientific and Technical Information (STINFO)—All technical publications and documents generated by Air Force-funded research, development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports that the DoD could decide to disseminate to the public domain.

Scintillations—In radio communications, rapid fluctuations in the strength of the (received) radio frequency signal due to atmospheric, manmade, or natural interferences or effects.

Screen—The face of a video display tube that displays an image or data.

Seamless Environment—In communications, an electronic environment that allows data to be accessed by the warfighter without regard to physical or electronic boundaries.

Seamless Operations—End-to-end automation and procedures that integrate all command, control, communications, computers and intelligence (C4I) elements and networks into an interoperable and cohesive global network that is transparent to the warrior.

Search Engine—A tool used to search the Internet for a particular subject or topic.

Secondary Channel—In a system in which two channels share a common interface, a channel that has a lower data signaling rate capacity than the primary channel.

Secondary Frequency Standard—A frequency standard that does not have inherent accuracy, and therefore must be calibrated against a primary frequency standard. (Secondary standards include crystal oscillators and rubidium standards.)

Secure Sockets Layer (SSL)—A security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Selective Fading—That type of fading in which the components of the received radio signal fluctuate independently.

Semi-Duplex—A method of operating a communications circuit where one end is duplex and the other end is simplex. Sometimes used in mobile systems with the base station being duplex and the mobile station being simplex.

Semiconductor—A material (element or compound) that displays a different electrical resistance in opposite directions of current flow. It has a higher resistivity than a conductor, but a lower resistivity than an insulator. Semiconductor materials are the basis of diodes, transistors, thyristors, photodiodes and integrated circuits.

Sensitive Information—The loss, misuse, unauthorized access to, or modification of information which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 522a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of the national defense or foreign policy. Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the *Computer Security Act of 1987*.

Sensitivity—In a radio receiver, the minimum input signal required to produce a specified output signal having a specified signal-to-noise ratio.

Serial—The handling of one item after another in a single facility such as transfer or store in a digit-by-digit time sequence or to process a sequence of instructions one at a time.

Serial Line Internet Protocol (SLIP)—Similar to Point-to-Point Protocol (PPP). SLIP is another standard protocol used to run TCP/IP over serial lines, such as telephone circuits or RS-232 cables. Unlike PPP, SLIP does not work on a LAN connection. SLIP is a popular way for dial-up users to access the Internet over conventional telephone lines.

Serial Transmission—The transmission in a sequence, over a single line, of individual signal elements. The sequential elements may be transmitted with or without interruption, provided they are not transmitted simultaneously.

Series of Records—A group of related records having a distinct title, application, and disposition schedule.

Server—A computer network device that provides service to the network users by managing shared resources.

Service Software—In computer programming, software designed specifically for service and repair work.

Shaping Network—A network inserted in a circuit for improving the wave shape of the signals.

Shared Data Field—A field contained within a record, defined to occupy the same record positions with more than one data element.

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Shell—An outer layer of an operating system that provides a menu-driven or graphical user interface, or the user's way of commanding the computer. Instead of presenting the user with a command line prompt, the shell presents a list of programs from which the user can choose.

Shift Register—In computing, a storage device, usually in a central processing unit, in which device a serially ordered set of data may be moved, as a unit, into a discrete number of storage locations.

Ship Earth Station—A mobile satellite Earth station in the maritime mobile satellite service located onboard ship.

Shop, Closed—The operation of a computer facility where programming service to the user is the responsibility of a group of specialists. The programmers are not allowed in the computer room to oversee the running of their programs.

Shop, Open—The operation of a computer facility where computer programming, coding, and operation can be performed by any qualified employee of the organization. Programmers may be in the computer room to oversee the running of their programs.

Short Title—This is the type of publication or form and its number. It is shown in the index of publications and forms in column 1. Examples are: AFPD 33-1, AFI 10-123, , AFVA 12-1, AF Form 909, DD Form 3152-6, TA 006.

Shortwave (Radio)—Pertaining to radio waves with a frequency above the medium frequency range (i.e., above 3 MHz), corresponding to wavelengths that are less than 100 meters. **NOTE:** The term **Shortwave** is not officially recognized by the international community.

Side Lobe—In a directional antenna radiation pattern, a lobe in any direction other than that of the main lobe.

Sideband—In radio communications, a band of frequencies of a transmitted (radio frequency) signal above and below the carrier frequency, produced by the modulation process.

Sideband Transmission—That method of transmission in which frequencies produced by amplitude modulation occur above and below the carrier frequency. The frequencies above (higher than) the carrier are called upper sideband; those below (lower than) the carrier are called lower sideband. The two sidebands may carry the same or different information. The carrier and either sideband may be suppressed independently. In conventional amplitude modulation both sidebands carry the same information and the carrier is present.

Sidetone—In telephone communications, the sound of the speaker's own voice (and background noise) as heard in the speaker's telephone receiver.

Signal—1. As applied to electronics, any transmitted electrical impulse. 2. Operationally, a type of message, the text of which consists of one or more letters, words, characters, signal flags, visual displays, or special sounds with pre-arranged meaning, and which is conveyed or transmitted by visual, acoustical, or electrical means.

Signal Compression—In analog (usually audio) communications systems, the reduction of the dynamic range of a signal by controlling it as a function of the inverse relationship of its instantaneous value relative to a specified reference level. Signal compression is used, amongst others, to improve signal-to-noise ratios, prevent overload of succeeding elements of a system, or to match the dynamic ranges of two devices.

Signal-To-Noise (S/N) Ratio—1. The ratio of the amplitude of the desired signal to the amplitude of the (unwanted) noise signals at a given point in time, expressed in decibels. 2. The amount by which a signal exceeds the circuit noise on a line over which it is transmitted.

Signaling—1. The use of signals for communication. 2. The method of conveying the signals over the circuit. 3. The exchange of information (other than by speech) specifically concerned with the establishment and control of connections and management in a communications network.

Simple Network Management Protocol (SNMP)—A standard network management service that provides a means of monitoring and managing bridges, hubs, servers, and routers.

Simplex Circuit—A circuit using ground return and affording communications in either direction, but only in one direction at a time. The circuit may be a single wire with ground return, or may be derived from the center of a balanced two-wire circuit and ground return.

Simplex Operation—That type of operation that permits the transmission of signals in either direction alternately.

Simulation—The representation of selected characteristics of the behavior of one physical or abstract system by another system. In a digital computer system, simulation is done by software; for example, (a) the representation of physical phenomena by means of operations performed by a computer system, and (b) the representation of operations of a computer system by those of another computer system.

Simultaneous Access—The process of obtaining information from or placing information into storage where the time required for such access depends on the simultaneous transfer of all elements of a word given storage location.

Singing—An undesired, self-sustaining audio oscillation in a circuit, usually caused by excessive gain in the circuit, unbalance of the hybrid termination, or combination thereof.

Single Sideband (SSB) Transmission—A transmission where only one sideband is transmitted, but the carrier frequency is present.

Single Sideband Suppressed Carrier (SSB-SC) Transmission—A generally amplitude modulated radio signal consisting of one sideband only (upper or lower) and in which the carrier frequency also has been suppressed (filtered out) to the point where it is insufficient to be demodulated in the receiver.

Site License Agreement—A contractual agreement with a commercial software business allowing use of their software product at a specific site or by a specific group of users. Contracts typically provide free or inexpensive upgrades and allow sharing software with multiple users at less cost than buying individual copies.

Site Preparation—Site preparation of a communications facility includes modifying facilities, surveying sites, and determining allied support costs.

Skip Distance—In radio transmission, the minimum distance between the transmitting station and the point of return to the Earth of the transmitted wave reflected from the ionosphere.

Skip Zone—A roughly coned-shaped region within the transmission range where signals from a transmitter are not received. It is the area between the farthest points reached by the ground wave and nearest points at which the refracted sky waves come back to Earth.

Sky Wave—A transmitted radiowave that travels upward from the antenna. Depending on its frequency, a sky wave may be reflected back to Earth by the ionosphere.

Slot Antenna—A radiating element formed by a slot in a conducting surface or in the wall of a waveguide.

Small Computer—A data processing system which can execute various programs. It usually consists of a keyboard, peripheral storage device, visual display device, printer, and central processing unit with random-access and read-only memory. A small computer may be operated stand-alone or networked with other computers. Personal computers, microcomputers, text processors, intelligent typewriters, and portable computers are all examples of small computers.

Small Computer Support Center (SCSC)—The base focal point for small computer support. This function is normally in the base communications organization.

Smooth Earth—Idealized surfaces, such as water surfaces or very level terrain, having radio horizons that are not formed by prominent ridges or mountains, but are determined solely as a function of antenna height above ground and the effective Earth radius.

Social Engineering—A deception technique utilized by hackers to derive information or data about a particular system or operation.

Society for Computer Simulation (SCS)—A professional society devoted primarily to the advancement of simulation and allied computer arts in all fields. The purpose of SCS is to facilitate communications among practitioners in the areas of computer simulation and mathematical modeling. SCS has worldwide membership and is a member of the American Federation of Information Processing Societies and the American Automatic Control Council.

Soft Keys—Visual representation of key functions on a display screen. This is usually associated with software controlled function key capabilities.

Soft Metric—Metric equivalents calculated by mathematical conversion of inch-pound measurements for specifications, standards, supplies, and services. The physical dimensions are not changed.

Software—A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (e.g., compilers, library routines, manuals, and circuit diagrams).

Software Engineering—The discipline devoted to the design, development, and use of software.

Software Portability—The ease with which software can be transferred from one information system to another.

Software Support—The sum of all activities that take place to ensure that implemented and fielded software continues to fully support the operational mission of the system. Software support includes pre- and post-deployment support.

Source Agency—A Federal, state, or local government agency that discloses records for the purpose of a computer match.

Source Code—A file of high-order or assembly language statements, usually containing comments and easily readable steps, which will be compiled or assembled to produce object code for a computer to execute. Modification and debugging of programs are done on source code.

Space Diversity—In radio communications, a method of transmission and, or reception employed to minimize the effects of fading by the simultaneous use of two or more antennas spaced a number of wavelengths apart.

Space Junk—In satellite communications, satellites that are still in orbit, but are no longer operating.

Space Operation Service—A radio communications service concerned exclusively with the operation of spacecraft, particularly space tracking, space telemetry, and space telecommand. These functions will normally be provided within the service in which the spacecraft is operating.

Space Radio Communications—Radio communications involving the use of one or more space stations, satellites, or other objects in space.

Space Station—A station located on an object which is beyond, is intended to go beyond, or has been beyond, the major portion of the Earth's atmosphere.

Space Subsystem—In satellite communications, that portion of the satellite link that is in orbit.

Space System—All of the devices and organizations forming the space network. The network includes spacecraft, ground control stations, and associated terminals.

Space Telemetry—The use of telemetry for the transmission from a space station of results of measurements made in a spacecraft, including those relating to the functioning of spacecraft.

Spare Parts—Reparable components or assemblies used for maintenance replacement purposes in major end items of equipment.

Spares—A term used to denote both spare and repair parts.

Special Intelligence Communications (SPINTCOM)—A dedicated family of circuits, terminals, and facilities that serve the special security office functions at most major headquarters worldwide.

Specification—A document that prescribes, in a complete, precise, verifiable manner, the requirements, design behavior, or characteristics of a system or system component.

Spectrum Designation of Radio Frequencies—A method of referring to a range or band of radio frequencies. The following are the frequency designations and ranges:

Table A1.1. Radio Frequencies.

Extremely Low Frequency (ELF):	below 30 Hz
Super Low Frequency (SLF):	30 to 300 Hz
Ultra Low Frequency (ULF):	300 to 3000 Hz
Very Low Frequency (VLF):	3 to 30 kHz
Low Frequency (LF):	30 to 300 kHz
Medium Frequency (MF):	300 to 3000 kHz
High Frequency (HF):	3 to 30 MHz
Very High Frequency (VHF):	30 to 300 MHz
Ultra High Frequency (UHF):	300 to 3000 MHz
Super High Frequency (SHF):	3 to 30 GHz
Extremely High Frequency (EHF):	30 to 300 GHz
Tremendously High Frequency (THF):	300 to 3000 GHz

Spectrum Management—Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Specular Reflector—Reflecting light in a diffuse manner.

Speech Synthesis—The generation of machine voice by arranging phonemes (e.g., *k, ch, sh,* and so forth) into words. Speech synthesis performs real-time conversion without a predefined vocabulary, but does not create human-sounding speech. Although individual spoken words can be digitized into the computer, digitized voice takes a lot of storage, and the resulting phrases lack inflection.

Splice Loss—In optical fiber systems, any loss of optical power at a splice.

Splice Organizer—In optical fiber systems, a device that facilitates the splicing or breaking out of optical cable. The organizer provides means to separate and secure individual buffer tubes and, or fibers or pigtails. It also provides the means to secure mechanical splices or protective sleeves used in connection with fusion splices, and contain the slack fiber that remains after the splicing process is completed.

Spread Spectrum—1. In general, a signal with a large time-bandwidth product. 2. A telecommunications technique in which the modulated information is transmitted in a bandwidth considerably greater than the frequency content of the original information. In satellite communications, spread spectrum may be employed as an anti-noise signal-gain processing tool.

Spread Spectrum System—A system that produces a signal with a bandwidth much wider than the intelligence or message bandwidth.

Spurious Emission—Emissions on frequencies that are outside the necessary bandwidth, the level of which may be reduced without affecting the corresponding transmission of information. Spurious emissions include harmonic emissions, parasitic emissions, intermodulation products, and frequency conversion products, but exclude out-of-band emissions.

Spurious Response—Any response of an electronic device to energy outside its designated reception bandwidth.

Squelch—In amplitude modulation radio communications, a circuit function in the receiver that acts to suppress the undesired noise or audio output of a receiver. The squelch function is activated in the absence of a sufficiently strong desired radio frequency input signal to exclude undesired lower-power radio frequency input signals that may be present at or near the desired frequency signal.

Staff Support—That part of the information management career field that provides executive and information management support within an organization, such as the information managers on the commander's staff and the information managers assigned to individual units or offices. Those services or processes performed by staff support information managers.

Stand-Alone Computer—A small computer able to provide processing capabilities independent of another computer.

Standard—1. An exact value, a physical entity, or an abstract concept established and defined by authority, custom, or common consent to serve as a reference, model, or rule in measuring quantities or qualities, establishing practices or procedures, or evaluating results. 2. A fixed quantity or quality.

Standard Frequency Service—A radio communications service for scientific, technical, and other purposes, providing the transmission of specified frequencies of stated high precision intended for general reception.

Standard Publication—Doctrine documents, policy directives, instructions, mission directives, manuals, indexes, directories, handbooks, catalogs, operating instructions, supplements, pamphlets, visual aids, bulletins, and staff digests.

Standard Table—Column heads run across the page and the information in each column runs down the page.

Standard Tactical Entry Point (STEP)—The STEP is a communications gateway that provides reachback into the Defense Information Systems Network (DISN) for deployed commanders. The STEP provides information (classified and unclassified) interchange, including voice, data, video, imagery, and message services (including the Automatic Digital Network and Defense Message System) from the deployed location via military satellite communications into the DISN.

Standards—The criteria described in a desired end result. A description of a level of attainment used as a measure of adequacy.

Standards Profile—See Profile.

Start-Stop System—See Asynchronous System.

Station Battery—A separate battery power source within a communications facility that provides direct current power for all significant requirements associated with the facility.

Station Clock—A clock that controls some or all of the equipment in the station that require local time control.

Station Load—The total (alternating current) electrical power requirements of the integrated station facilities.

Statistical Multiplexing—Multiplexing in which channels are established on a statistical basis (i.e., connections are made according to probability of need).

Storage—1. Maintaining information for later retrieval and access by the user. 2. Pertaining to a device into which data can be entered, held, and retrieved.

Store-and-Forward Message System—The communications process that allows messages to be stored at intermediate nodes before being forwarded to their destination.

Stovepipe System—A dedicated or proprietary system that operates independently of other systems. The stovepipe system often has unique, nonstandard characteristics.

Structured Query Language (SQL)—A data base language. It is a unified language that allows data definition, manipulation, and control. The language was developed to access relational data bases.

Subaccount Representative (SAR)—A customer to the customer account representative (CAR). This person is at a lower level in the unit, such as a branch. A SAR submits requirements and requisitions to the CAR.

Subcarrier—In frequency division multiplexing, a carrier used to modulate another carrier. The resultant modulated carrier can be used to modulate another carrier, and so on, so that there can be several levels of subcarriers or intermediate carriers.

Sublayer—In a layered open communications system, a specified subset of the services, functions, and protocols included in a given layer.

Subnetwork—A collection of equipment and physical transmission media that forms an autonomous whole and that can be used to interconnect systems for the purposes of communication.

Subroutine—A sequence of instructions that tell the computer to perform a specific task. This sequence of instructions is usually considered as a separate routine. It may also be a part of a larger routine that can be compiled separately, but usually cannot be run as a separate program.

Subscriber—In a public telecommunications network, the ultimate user, i.e., the customer, of a communications service. Subscribers include individuals, activities, organizations, etc. Subscribers use end instruments, such as telephones, modems, facsimile, computers, and remote terminals. Subscribers do not include communications systems operating personnel, except for their personal terminals.

Supervisory Signals—Signals used to indicate and, or control the various operating states of the circuits and, or equipment assemblies of a communications system.

Supplement—A document that adds material to a publication a higher headquarters issues.

Supplementation—The publication by the DoD components of directives, instructions, regulations, and related documents that adds to, restricts, or otherwise modifies the policies and procedures of DoD issuances.

Supraordinate Window—A higher level window, usually the window from which subordinated options or tasks are controlled.

Surface Acoustic Wave (SAW)—When used in the context of touch screen technology, an approach that uses ultrasonic sound beams transmitted from two perpendicular sides of a display frame.

Surface Wave—In radio communications, radio frequency waves that propagate close to the surface of the earth. Synonym: **Ground Waves**.

Surveillance Television (STV)—A closed-circuit television system that provides a visual representation of secure and hazardous areas for remote monitoring.

Switched Multi-Megabit Data Service (SMDS)—A high speed (1.544 Mbps to 45 Mbps), connectionless, packet-switched service allowing local area network-like performance and features over a metropolitan or wide area network. SMDS is not a protocol, but rather a service that operates independently of the underlying protocol. SMDS is a stepping stone to asynchronous transfer mode (ATM) because of its forward compatibility with ATM and compatibility with frame relay.

Symbolic Language—A computer programming language used to express addresses and instructions with symbols convenient to humans rather than to machines.

Synchronous—Having a constant-time interval between successive bits, characters, or events.

Synchronous Optical Network (SONET)—A set of specifications and concepts for high speed optical transport over fiber multiplexed systems. It has the distinct advantage of providing (a) a standardized optical interface and signaling format across all fiber systems, (b) advanced maintenance and network management features, and (c) easier add-drop multiplexing for network inter-connections and rearrangements. SONET deployment can increase network survivability.

Synchronous Orbit—An orbit in which a satellite has a velocity synchronized to the speed of the rotation of the Earth and thus remains above a fixed point on the Earth’s surface. This occurs at an altitude of approximately 22,300 miles over the equator.

Synchronous Satellite—A satellite in a synchronous orbit.

Synchronous System—A system in which the transmitter and receiver are operating in a fixed time relationship.

Synchronous Transmission—1. A form of data transmission in which transmitting and receiving stations are synchronously timed to eliminate the need for stop-and-start bits. 2. A transmission process such that between any two significant instants in the overall bit stream, there is always an integral number of unit intervals. Compare with Asynchronous Transmission.

Syntonization—In communications-electronics, the process of setting the frequency of one oscillator equal to that of another.

System—Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

Systems Architecture—A description, including graphics, of systems and interconnections providing for, or supporting warfighting functions. The systems architecture shows how multiple systems link and interoperate, and may describe the internal construction and operations of particular systems within the architecture. For the individual system, the system architecture includes the physical connection, location, and identification of key nodes (including material item nodes), circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters (e.g., mean-time-between-failure, maintainability, availability, etc.).

System Control—In satellite communications, system control of communications satellites embodies several different control functions that are accomplished by different levels or types of commands and which may be done by the same or separate control facilities. Control functions relate to: (a) Operational Control. The control exercised to determine the location of satellites, the location of fixed Earth terminals, and the parameters required for operation of the Earth segment, such as allocation of satellite power, bandwidth, access time, and operating frequencies (channels); (b) Satellite Communication Control. The control of a satellite exercised by a master station to ensure that the Earth segment operates within its assigned parameters and according to prescribed procedures; (c) Satellite Control. The manipulative control and monitoring of onboard subsystems and components of a satellite, including those affecting position and attitude as well as the adjustment and switching of subsystems or components.

System Management Services—System management services support all activities dealing with the management of the computing environment, interacting with all other generic technology environments to provide the management capability to monitor and control the total environment.

System Manager—1. A general term of reference to those organizations directed by individual managers exercising authority over the planning, direction, and control of tasks and associated functions essential for support of designated weapons or equipment systems. The authority vested in this organization may include such functions as research, development, procurement, production, materiel distribution, and logistics support, when so assigned. 2. The official who is responsible for managing a system of records, including policies and procedures to operate and safeguard it. Local system managers operate record systems or are responsible for part of a decentralized system.

System Notice—The official public notice published in the *Federal Register* of the existence and content of the system of records.

System of Records—A group of records containing personal information retrieved by the subject's name, personal identifier, or individual identifier through a cross-reference system.

System of Systems—A concept that describes the need for a degree of interoperability among all Air Force communications and computer systems because all information generated is eventually consolidated (through the hierarchy of communications and computer systems) to support the overall Air Force mission.

System Security Authorization Agreement (SSAA)—The SSAA is the depository for evidence showing a system meets the system security policy requirements, that all certification tasks are completed, the system is approved to operate, and a plan exists for maintaining the security posture/ accreditation.

System Services—Firmware and software that provide an aggregation of network element functions into a higher level function and provide an interface to the data contained in the system.

System Software—Application-independent software that supports the running of application software and manages the resources of the application platform.

System Software (Basic or Nonfunctional)—Routines and programs designed to extend or facilitate the use of particular automated equipment. As a rule, the vendor provides system software. It is usually essential for the system operation. Examples of systems software are executive and operating systems, diagnostic programs, compilers, assemblers, utility routines (such as sort-merge and input or output conversion routines), file management programs, and data management programs.

Systems Control—In telecommunications, a set of processes, procedures, hardware, automated data processing equipment, communications, and personnel to perform a specific set of subfunctions that consist of facility surveillance, traffic surveillance, network control, traffic control, and technical control.

Systems Design—A process of defining the hardware and software architecture, components, modules, interfaces, and data for a system to satisfy specified requirements.

Systems Telecommunications Engineering Manager (STEM)—A C4 systems engineer who provides technical engineering planning services in support of C4 systems and base infrastructures. The base-level STEM (STEM-B) has technical responsibility for engineering management and assists the base communications and information systems officer in system engineering and configuration control. The command-level STEM (STEM-C) provides technical assistance to the major commands (MAJCOM) and coordinates with STEM-Bs on future MAJCOM mission changes, programs, and efforts at the MAJCOM level.

T-Carrier System—A digital data carrier system that may be submultiplexed in many different ways to provide both analog and digital data services. If the T is preceded by an F, fiber optic cable system is indicated using the same rates. Common United States examples are: T1 that operates at 1.544 Mbps, T1C that operates at 3.152 Mbps, T2 that operates at 6.312 Mbps, T3 that operates at 44.736 Mbps, and T4 that operates at 274.176 Mbps. T-carrier systems were originally designed to transmit digitized voice signals. Current applications also include digital data transmissions. The designators for T-carrier in the North American digital hierarchy correspond to the designators for the digital signal level hierarchy.

Table—Asystematic listing of information in columns or rows used to explain, clarify, or replace narrative text in a publication.

Tactical Communications System—A system configured by various types of fixed sizes, self-contained assemblages (radio repeater and terminal equipment, switching, interconnect and control facilities, etc.) which are organic to the tactical forces and designed to meet the requirements of ever changing tactical situations.

Tactical Switchboard—This switchboard operates independently from the base switchboard and provides telephone service for designated subscribers for command and control and other combat-essential purposes. In many cases the tactical switchboard is collocated with the base switchboard to keep the number of switchboard attendants at a minimum.

Tag Image File Format (TIFF)—In computer graphics, a file format used to store an image using the particular data structure of the file.

Tandem—1. The connection of the output terminals of one network, circuit, or link, directly to the input terminals of another network, circuit, or link (e.g., a microwave radio relay system employs tandem links). 2. A telecommunications switching arrangement whereby the trunk from a calling switch is connected to the trunks of a called switch through one or more intermediate switches which are referred to as "tandem switches" or "network tandems."

Target Architecture—The definition of the architecture components and their key attributes needed to support an organization over an agreed-upon planning interval (usually 3-5 years). It must be consistent with the organization’s long-term objectives.

Tariff—Rates or charges for a business or public utility by commercial telephone companies and filed with a public regulatory agency.

Technical Architecture—A minimal set of rules governing the arrangement, interaction and interdependence of system parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Technical Architecture Framework for Information Management (TAF—IM) A Defense Information Systems Agency Center for Architecture multi-volume publication that provides guidance for the evolution of the DoD technical infrastructure. The TAFIM does not provide a specific system architecture. It provides the services, standards, design concepts, components, and configurations that can be used to guide the development of technical architectures that meet specific mission requirements. The TAFIM applies to information system technical architectures at all DoD organization levels and environments (tactical, strategic, sustaining base). The TAFIM uses Federal and National standards adopted by industry and international standards accepted worldwide by United States allies.

Technical Control Facility (TCF)—A physical plant, or a designated and specially configured part thereof, containing the necessary distribution frames and associated panels, jacks, and switches; monitoring, test, and conditioning equipment; and orderwire/service channel communications to enable technical control personnel to exercise essential operational control over communications systems. Technical control includes the real-time transmission system configuration control, quality assurance, quality control, alternate routing, patching, testing, directing, coordinating, restoring, and reporting functions necessary for effective maintenance of transmission paths and facilities.

Technical Data Package (TDP)—A technical description of an item adequate for supporting an acquisition strategy, production, engineering, and logistics support. The description defines the required design configuration and procedures to ensure adequacy of item performance. It consists of all applicable technical data, such as drawings, associated lists, specifications, standards, performance requirements, quality assurance provisions, and packaging details.

Technical Information—Information, including scientific information, that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

Technical Interface—The functional, electrical, and physical characteristics necessary to allow the exchange of information across an interface between different C4I systems or equipment. Includes Technical Interface Standards.

Technical Interface Standards—Specifications for functional, electrical, and physical characteristics necessary for exchanging information across an interface between different tactical C4I systems or equipment.

Technical Load—The portion of the operational (electrical) load required for communications, tactical operations, and ancillary equipment including necessary lighting, air conditioning, or ventilation required for full continuity of communications.

Technical Manual (TM)—A publication that contains instructions for the installation, operation, maintenance, training, and support of weapon systems, weapon system components, and support equipment. Technical Manual information may be presented in any form or characteristic, including, but not limited to hard copy, audio and visual displays, magnetic tape, disks, and other electronic devices. A Technical Manual normally includes operational and maintenance instructions, parts lists or parts breakdown, and related technical information or procedures exclusive of administrative procedures. Technical orders that meet the criteria of this definition may also be classified as technical manuals.

Technical Reference Codes (TRC)—A compendium of interoperability references (policy, directives, transition guidance, and standards). TRCs have been developed for planning, acquiring, and implementing interoperable, scalable, and portable Air Force information technology systems, system components, and services.

Technical Reference Model (TRM)—A common vocabulary and set of services and interfaces common to DoD information systems. The associated standards profile identifies standards and guidelines in terms of the reference model services and interfaces. These standards and guidelines can be applied and tailored to meet specific mission area requirements.

Technical Solution—A detailed description of the hardware, software, data, connectivity, logistics support, and other resources necessary to provide the most cost-effective solution to correct a deficiency or shortfall in mission capability. It includes the recommended acquisition method and strategy, estimates of all one-time and recurring costs, identification of manpower requirements (additional or savings estimate), and a schedule of events.

Telecommunications—1. Any transmission, emission, or reception of signs, signals, writings, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems. 2. Transmitting, communicating, or processing information, including preparing such information by electrical, electromagnetic, electromechanical, or electro-optical means.

Telecommunications Service Order (TSO)—The authorizing and specifying order from the Defense Information Systems Agency to start, change, or discontinue circuits or trunks, or to effect administrative changes.

Telecommunications Service Request (TSR)—A validated message request for service that details the type of service, service locations, and other pertinent information required to specify parameters to the agency or commercial carrier providing the service.

Telecommunications System Standards (TCSS)—A standardization area of the Defense Standardization Program. This area establishes uniform engineering criteria for terminal equipment, transmission equipment and media, and switching equipment in military telecommunications interoperability with non-military systems that support military functions. Activities within the TCSS area include participating in Federal, commercial, and international standardization efforts as well as developing military unique telecommunications standards.

Teleconference—A conference between persons remote from one another but linked by a telecommunications system.

Telegraph—A system of communication using coded signals.

Telemetry—The use of telecommunications for the transmission of information on measurements. The outputs from counters or sensors are carried, usually via line-of-sight microwave radio links, to a station or facility where the signals can be recorded and, or analyzed.

Teleprocessing—1. Data processing using computers and communications facilities. 2. A combination of telecommunications and computer operations that interact in the automatic processing, reception, and transmission of data or information.

Telnet—The Internet standard protocol to connect to remote terminals.

Template—1. A document that describes a customer's operational architecture (information flow) and provides an as-is (baseline) and to-be systems architecture using DoD, Air Force, and other applicable technical architectures in the recommended solutions. A template ties operational, system, and technical architectures together for the customer based on the customer's specified area of interest (i.e., a specific system, process, and, or facility). The template is customer focused. 2. A form displayed on a computer monitor into which you enter data for processing.

Tera (T)—A prefix used to denote trillion (1012).

Terahertz (THz)—A unit denoting one trillion hertz.

Terminal—An input or output device, usually a monitor and keyboard, through which you enter data into or extract data from a computer.

Terminal Equipment—Communications equipment at each end of a circuit or channel to permit the stations involved to accomplish the purpose for which the circuit or channel was established.

Test Tone—In the testing of telephone or audio circuit/channels, a standard tone of 1000 hertz at 1 megawatt of power that can be sent on a circuit to locate trouble or serve as a reference for adjustment of signal levels over a communications system.

Text Documents—Narrative or tabular documents, such as letters, memoranda, and reports, in loosely prescribed form and format.

Text Table—Column heads run down the page and the information for each head is entered beside the head. Column heads are usually repeated for each entry. Decision Logic Tables and Specified Action Tables are also considered tables.

Text-Based Systems—In computing, a method of organization in which the primary form of interaction between the system and user is through text rather than through graphical or voice interaction.

Thermal Noise—In communications-electronics. Random, undesirable electrical signals generated by thermal agitation of electrons in a conductor.

Tie-Line Service—Direct trunks between two telephone exchanges that have dial-to-dial termination. When a base or activity needs frequent telephone contact with another government agency or customer served by a different telephone exchange, direct tie-lines are usually more economical and convenient.

Time Division Multiple Access (TDMA)—In satellite communications, the use of time interlacing to provide multiple and apparently simultaneous to a single transponder with a minimum of interference.

Time Division Multiplexing (TDM)—The process or device in which each modulating wave modulates a separate pulse subcarrier, the pulse subcarriers being spaced in time so that no two pulses occupy the same transmission interval. Time division permits the transmission of two or more signals over a common path by using different time intervals for the transmission of the intelligence of each message signal.

Time Jitter—Short-term variations or instability in the duration of a specified interval.

Time Sharing—The interleaving in time of two or more independent processes on one functional unit.

Timing Signal—1. The output of a clock. 2. A signal used to synchronize interconnected equipment.

Toll Quality—The high correlation between the intelligibility and quality of electronically transmitted voice with that of the natural human voice.

Topology—The layout of nodes (switches, concentrators) and transmission paths of a network.

Touch Interactive Display (TID)—Uses a physical device between the user and the display that acts as the input mechanism.

Track—The portion of a moving storage medium, such as a drum, tape, or disk that is accessible to a given reading or writing station.

Traffic—The information moved over a communications channel. A quantitative measurement of the total messages and their length, expressed in hundred-character seconds (cluster control units) or other units, during a specified period of time.

Transaction Set—In electronic data interchange, the data sent by one trading partner to another that allows recipient to complete a single transaction, essentially a complete business document.

Transceiver—Combination of transmitter and receiver. An item of equipment, device, or circuit that can both transmit and receive signals (e.g., telephone, two-way radio). This term is sometimes also applied to a terminal with facilities for both sending and receiving messages.

Transient—An unpredictable short-duration change in circuit condition; a pulse or increase in circuit noise. An example is impulse noise in a communications circuit.

Transliteration—1. Code conversion; a change of the bit patterns used to represent the characters of a set. 2. A change in the representation of characters. 3. An erroneous substitution of one bit or character for another.

Transmission Facility—In telecommunications, a cable, radio, or satellite communications facility that provides a transmission medium for DSN interswitch trunks and access lines.

Transmit Clock—The clock (timing signal source) from which the transmitting circuitry of a modem obtains its timing.

Trap Door—A hidden software or hardware mechanism that responds to a special input that is used to circumvent security controls.

Tremendously High Frequency (THF)—Frequencies of electromagnetic waves in the range of 300 to 3000 gigahertz.

Tributary Station—Also slave station, secondary station, or data station. In a data network, a station other than the master station.

Tropospheric Scatter (Communications)—A type of wideband radio communications that uses the troposphere to scatter and reflect the radio waves, thus providing communications between stations that are not in line-of-sight. Tropospheric scatter links operate in the ultra high frequency range for distances up to 600 miles. Once a popular long-haul communications method, most fixed tropospheric scatter links have been replaced by satellite communications.

Truncate—To remove leading or trailing digits from a number without regard to the effect on the remaining digits.

Trunk—1. A single transmission channel between two points, both of which are switching centers or nodes, or both. 2. In a telephone system, a multiple circuit connection between two exchanges. 3. A communications channel between two different offices or between groups of equipment within the same office.

Trunk Exchange—The elements of a telephone exchange that perform the interconnection of trunks.

Trunking—In land mobile radio (LMR), trunking is defined as the automatic time-sharing of a small number of frequency resources (channels) to serve a large number of users. The relatively short duration of an individual LMR call can allow channels of a trunked LMR system to be shared in a very spectrum-efficient manner. Trunking systems offer more flexibility than conventional non-trunked systems.

Turnkey System—A complete (computer) system designed for a specific user. A term applied to a contract or operation in which the prime contractor designs, installs, and tests a complete system and delivers it in an operating condition.

Twisted Pair—Two insulated wire conductors twisted together for use as a telephone or data communications circuit. The twist improves the transmission performance of the resulting circuit. Individual twisted pairs are usually cabled together with other twisted pairs to form twisted pair cables.

Two-Wire Line—In telecommunications, a two-conductor circuit used for one-way or two-way transmission.

Type Designation—A specific combination of letters and numerals, structured in accordance with Military-Standard (MIL-STD) 196, *Joint Electronic Type Designator (JETD) System*, that provides a standard means of uniquely identifying electronic equipment by design configuration (e.g., AN/TRC-97).

Type-Ahead—Capability of the computer to receive commands faster than it can display their results.

Ultra High Frequency (UHF)—Frequencies of electromagnetic waves in the range from 300-3000 megahertz.

Ultra Low Frequency (ULF)—Frequencies of electromagnetic waves in the range from 300-3000 hertz.

Unbalanced Line—In telecommunications, a transmission line in which the magnitudes of the voltages on the two conductors are not equal in respect to ground (e.g., a coaxial line).

Uniform Resource Locator (URL)—An Internet "address" of a resource. On the World Wide Web, URLs represent hypermedia links and links to network services within Hypertext Markup Language documents. A URL can represent nearly any file or service on the Internet. The first part of the URL specifies the method of access; the second is typically the address of the computer where the data or service is located; further parts may specify names of files, port to which to connect, or the text to search for in a data base.

Unintelligible Crosstalk—Crosstalk given rise to unintelligible sounds.

Uninterruptible Power Supply (UPS)—In computing, a device inserted between a power source and a system to ensure that the system is guaranteed a precise, uninterrupted power supply, irrespective of variations in the power source voltage.

Unipolar—In data communications, pertaining to a signal that has excursions from zero to either a positive or negative value, but not both. (e.g., consists of a stream of positive pulses only).

Unit of Requisition (UR)—An abbreviation that shows the construction of a form. Some examples are: CS (cut sheet), ST (set), TG (tag).

UNIX—A general purpose, multi-user operating system suitable for use in a wide range of computers. Developed by Bell Laboratories in 1969, it has become a de facto industry standard and is available on a wide range of hardware systems from a variety of vendors.

Unofficial Commercial Service—Telephone service that directly connects private telephones to a commercial telephone exchange. Not required for conduct of official business. This includes telephone service in military housing, non-appropriated fund facilities, commercial activities, and other facilities.

Unscheduled Maintenance—Also referred to as Corrective Maintenance, includes all maintenance actions to restore an item of equipment or system to a specified condition as a result of a failure.

Unscheduled Record—A record whose disposition is waiting on the National Archives and Records Administration's final approval.

Uplink—In satellite communications, that portion of a communications link from the earth terminal to the satellite.

U.S. Government Optional Forms—These forms bear the designation Optional Form or OF. Two or more Federal agencies may develop an optional form to eliminate separate agency forms for similar purposes. General Services Administration, Office of Information Systems, approves optional forms for non-mandatory use by Federal agencies.

U.S. Government Standard Forms—These forms bear the designation Standard Form, Stock Form, or SF. A federal agency prescribes these forms under its authority. The General Services Administration, Office of Information Systems, also approves them for mandatory use by Federal agencies. The regulations of the issuing agency normally include the mandatory use of these forms.

User—1. A person or organizational unit responsible for applying an automated or manual procedure to support the execution of a process. 2. Any person, organization, or functional unit that uses the services of an information processing system.

User Friendly—Designating a computer, terminal, program, and so forth, that is easily used and understood by a wide variety of people.

User Interface—In man-machine interfaces, the interface through which the user and a system or computer communicate. It includes input and output devices, such as a keyboard, printer, and display, and also the software-controlled means by which the users are prompted to supply data needed by the application, and by which they are notified of their errors and how to correct them.

Utility Program—A computer program supplied for common routine tasks (e.g., copying files).

Variable Costs—Costs that rise and fall as production increases and decreases. Such costs include supplies, contract maintenance agreements, and some rentals. The manager should use care in cutting expenses in these areas, as it could drive costs up in other areas. For example, savings from bulk purchases of paper supplies can increase warehouse costs, and personnel costs to manage the stock. Buying inexpensive supplies that turn out to be of inferior quality can create equipment operating problems, reducing personnel productivity and increasing the total cost of production.

Very Low Frequency (VLF)—Frequencies of electromagnetic waves in the range of 3-30 kilohertz.

Vestigial Sideband (VSB) Transmission—In radio communications, a modified amplitude modulation transmission in which one sideband, the carrier, and only a portion of the other sideband are transmitted.

Video—Electronic recording and playback of imagery.

Video Random Access Memory (VRAM)—Random access memory that is used to hold data that defines an image displayed on the monitor.

Video Teleconferencing (VTC)—A telecommunications system that encompasses video, data, and voice components. VTC is a real-time electronic means of communicating visual, audio, and graphics information from one location to another, or among multiple locations. VTC may also include teletraining or distance learning to provide interactive remote site training.

Virtual—A term used in various ways to indicate that the actual physical implementation (storage, peripheral device, communications circuit) is different from that perceived by a user or user program.

Virtual Disk—In memory systems, an area of main storage in which the data is structured as if it were stored on a floppy disk.

Virtual Memory—In computer memory systems, this term describes memory or a computer storage location that is used to simulate another type of memory or storage even though it does not physically exist. It is a technique that allows the processor to employ its full address space although it exceeds the physical main memory available. The virtual memory space exists on the disk, when the processor addresses a portion of its address space outside the main memory, special hardware locates the required page on the disk and transfers it to a section of the main memory.

Virtual Network—A network that provides virtual circuits and that is established by using the facilities of a real network.

Virtual Reality (VR)—Computer-generated images and sounds representing real-world environments. VR is an interactive technology that creates the illusion that one is immersed in a world created by the computer (program). It is fundamentally a communications medium that transforms information from a computer to a person through the senses. VR systems place the user in an artificial environment that the user can manipulate.

Virtual Reality Modeling Language—A draft specification for the design and implementation of a platform independent language for virtual reality scene description.

Virtual Terminal—The ability for terminal systems and host applications on a network to communicate without requiring either side to know the terminal characteristics of the other; provides an implementation-independent and interoperable teletype function capable of a simple character/lines dialog, and also a forms capability intended to support forms-based applications with local entry. It can speed up the operation of microcomputer software that is designed to extract its data from a floppy disk.

Vision—An overarching statement or decision of the way an organization wants to be. An ideal state of being at a future point. This is a compelling description of what an organization will look like and how it will operate when accomplishing its mission in a way consistent with its values, guiding principles, and ideals.

Visual Information (VI)—Use of one or more of the various visual media with or without sound. Generally, VI includes still photography, motion picture photography, video or audio recording, graphic arts, visual aids, models, display, visual presentation services, and the supporting processes.

Visual Information (VI) Documentation (VIDOC)—Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, usually not controlled by the recording crew.

Visual Information (VI) Products—VI media elements such as still photography (photographs, transparencies, slides, and filmstrips), audio and video recordings (tape or disk), graphic arts (including computer-generated products), models, and exhibits. VI production is a unique form of VI product and usually is addressed separately.

Visual Information Support Center (VISC)—VI activities that provide general support to all installation, base, facility, or site organizations or activities. Typically, VISCs provide laboratory support, graphic arts, VI libraries, and presentation services.

Visual Information (VI) Systems—Visual information systems include still and motion picture photography, video and audio recording, video teleconferencing, graphic arts, base government-access channel television, visual aids and displays, visual presentation services, and supporting processes.

Vital Records—Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities.

Voice Frequency (VF) Channel—A transmission path or channel, normally part of a communications system, suitable for carrying analog signals and quasi-analog signals under certain conditions. In DoD communications systems, a VF channel accommodates input signals in the range of 300-3400 hertz.

Voice Recognition—The conversion of spoken words into computer text. Speech is digitized first then matched against a dictionary of coded wave forms. The matches are converted into text as if the words were typed on the keyboard. Speaker-dependent systems must be trained before using, by taking samples of actual words from the person who will use it.

Voice-Coder (Vocoder)—A device that usually consists of a speech analyzer which converts analog speech waveforms into narrowband digital signals, and a speech synthesizer which converts the digital signals into artificial speech sounds. Vocoders are used to reduce bandwidth requirements for transmitting digitized speech signals.

Volatile Memory—Memory that loses its stored data when power is removed.

Volume Unit (VU)—The unit of measurement for electrical speech power in communications work as measured by a VU meter. Zero VU equals zero dBm (1 milliwatt) in measurements of sine wave test tone power.

VOX—A voice-operated relay circuit that permits the equivalent of push-to-talk operation of a radio transmitter by an operator.

Waveguide—A transmission line comprised of a hollow metallic conductor generally rectangular, elliptical, or circular in shape, within which electromagnetic waves may be propagated.

Wavelength—The length of a electromagnetic or radio wave indicated in meters. It is equal to the distance traveled by the wave in one period of oscillation. Wavelength and frequency are directly related. The wavelength equals the velocity of the wave divided by its frequency.

Wavelength Division Multiplexing (WDM)—A technique that is identical to frequency division multiplexing. The term is applied to the use of different wavelengths for the light signals along an optical fiber.

White Noise—Noise whose frequency spectrum is continuous and uniform over a wide frequency range.

Wide Area Information Service (WAIS)—A distributed information service and search engine that allows natural language input and indexed searching. Many Web search utilities use a WAIS engine.

Wide Area Network (WAN)—A public or private computer network serving a wide geographical area. All network services offered by public network providers such as public and virtual private switched voice, switched and dedicated data, gateway and enhanced service offerings (e.g., AT&T, MCI, Internet, and so forth).

Wideband—Wideband has many meanings depending on its application. Wideband is often used to distinguish from Narrowband, where both terms are subjectively defined relative to the implied context: (a) The property of any communications facility, system, equipment, or channel, in which the range of frequencies used for transmission is greater than 0.1 percent of the midband frequency. (b) In telecommunications systems, a bandwidth exceeding that of a nominal 4 kilohertz telephone voice channel.

Wideband Modem—1. A modem whose modulated output signal can have an essential frequency spectrum that is broader than that which can be wholly contained within, and faithfully transmitted through, a voice channel with a nominal 4 kilohertz bandwidth. 2. A modem whose bandwidth is greater than that of a narrowband modem.

Wideband System—In telecommunications, a system with a multichannel bandwidth of 20 kilohertz or more.

Wing Command and Control System (WCCS)—A secure, automated, distributed wing-level command and control system that provides wing commanders and staff with timely information to support decisions. It automates information flow between the wing operations center and other wing-level, force-level, and base-level workcenters by consolidating data from supply, maintenance, operations, mission planning, intelligence, and weather information systems.

Word—In computing, a collection of bits treated as a single unit by the central processor.

Word Processing—The manipulation of textual material by a keyboard device capable of controlled storage, retrieval, and automated typing.

Workgroup Administration—A group of tasks that will provide immediate front-line support to local unit customers and provide the primary interface to the communications squadron when questions or problems are beyond local support capabilities.

Workstation—1. In automated systems, such as C4 systems, the input, output, display, and processing equipment that provides the operator-system interface. 2. A configuration of input, output, display, and processing equipment that constitutes a stand-alone system not requiring external access.

World Wide Web (WWW)—An international, virtual network-based information service composed of internet host computers that provide on-line information in a specific hypertext format. The WWW, called the Web for short, exists virtually and uses the internet to transmit hypermedia documents between computers internationally. No one organization owns the WWW; users are responsible for the documents they author and make available publicly on the Web. The Web refers to a body of information, while the Internet refers to the physical side of the Global network.

Worldwide Numbering and Dialing Plan (WNDP)—A standard numbering system that can serve all Defense Switched Network (DSN) users throughout the world in a uniform manner.

Worm—A computer program that replicates itself and is self-propagating; similar to a virus. While viruses are designed to cause problems on a local system and are passed through boot sectors of disks and through files, worms are designed to thrive in network environments.

Write—To transfer information to an output medium. To copy from internal storage to external storage.

Write Enable—In computer memory systems, a mechanism that enables data or signals to be recorded on a tape or disk. In the absence of this mechanism, the tape or disk is protected against any unwanted or accidental overwriting.

Write-Once Read-Many (WORM)—In computing, refers to a type of optical memory disk that can be written to once and cannot be erased or formatted.

X—1. A term used in publishing bulletins meaning Controlled Distribution. 2. A prefix for X.-series recommendations. X series standards are sets of data telecommunications protocols and interfaces defined by International Telegraph and Telephone Consultative Committee (CCITT) recommendations and range from X.-1 through X.-400 +.

X-Axis—A horizontal axis in a system of rectangular coordinates; that line on which distances to the right or left (east or west) of the reference line are marked, especially on a map, chart, or graph.

X-Y Plotter—In peripherals, a plotting device that receives X- and Y- coordinates from a computer and plots a coordinate graph.

Y-Axis—A vertical axis in a system of rectangular coordinates; that line on which distances above and below (north or south) the reference line are marked, especially on a map, chart, or graph.

Yagi Antenna—A directional antenna array usually consisting of one driven one-half wave length dipole section, one parasitically excited reflector, and one or more parasitically excited directors. A yagi antenna offers very high directivity and gain.

Yaw—In satellite communications, a rotation of a satellite about an axis that joins the satellite to the center of the Earth.

Z—In electronics, the symbol for Impedance.

Z-Axis Intercept—In satellite communications, the intersection of a satellite’s Z-axis and the earth’s surface. It defines an antenna’s pointing direction.

Zero A Device—To erase all the data stored in a memory. Synonymous with bit stuffing. The operation of inserting 0-bits in strings of 1-bits to prevent any groups in the user data stream from being interpreted as flags, or, possibly, control characters.

Zero Suppression—In computing, the elimination of zeros to the left of the most significant digits of a number, especially before printing.

Zero Transmission Level Point (0 dBm TLP)—In a communications system, a point in the signal path at which the reference signal power level is 1 milliwatt, that is, 0 dBm. The reference is for system design and test purposes; the actual power level of the communications traffic is not necessarily 0 dBm.

Zero-Level Decoder—A decoder that yields an analog level of 0 dBm at its output when the input is the digital milliwatt signal (a 1 kilohertz sine wave).

Zerofill—To fill unused storage locations (memory) with the representation of the character denoting 0.

Zip Cord—In optical communications, a two-fiber cable consisting essentially of two single-fiber cables having their jackets conjoined by a strip of jacket material.

Zone Beam—In satellite communications, a satellite beam pattern with a footprint that can cover less than 10 percent of the Earth’s surface.

Attachment 2

INFORMATION ASSURANCE TERMINOLOGY

Abbreviations and Acronyms

ACL—Access Control List

ACO—Access Control Officer

ACN—Accreditation Control Number

ACM—Access Control Mechanism

ADM—Advanced Development Model

AE—Application Entity

AIN—Advanced Intelligence Network

AIRK—Area Interswitch Rekeying Key

AISS—Automated Information System Security

AK—Automatic Remote Rekeying

AKDC—Automatic Key Distribution Center

AKD/RCU—Automatic Key Distribution/Rekeying Control Unit

AKMC—Automated Key Management Center

AKMS—Automated Key Management System

ALC—Accounting Legend Code

AMS—Auto-Manual SystemAutonomous Message Switch

AOSS—Automated Office Support Systems

APC—Adaptive Predictive Coding

APL—Assessed Products Listing

ASIM—Automated Security Incident Measurement

ASPJ—Advanced Self-Protection Jammer

ASSIST—Automated information system Security Incident Support Team

ASU—Approval for Service Use

CA—1. Controlling Authority
2. Cryptanalysis
3. COMSEC Account
4. Command Authority
5. Certification Authority

C&A—Certification and Accreditation

CAA—Controlled Access Area

CAP—1. Controlled Access Protection
2. Cryptographic Access Program

CAW—Certificate Authority Workstation

CCEP—Commercial COMSEC Endorsement Program

CCI—Controlled Cryptographic Item

CCO—Circuit Control Officer

CDS—Cryptographic Device Services

CE—Compromising Emanations

CEPR—Compromising Emanation Performance Requirement

CER—Cryptographic Equipment Room

CFD—Common Fill Device

CI—Critical Indicators

CIAC—Computer Incident Assessment Capability

CIK—Crypto-Ignition Key

CIP—Crypto-Ignition Plug

CIRK—Common Interswitch Rekeying Key

CIRT—Computer Security Incident Response Team

CK—Compartment Key

CKG—Cooperative Key Generation

CKL—Comprised Key List

CL—Certification Level

CLMD—COMSEC Local Management Device

CM—Countermeasure

CMCS—COMSEC Material Control System

CNCS—Cryptonet Control Station

CNK—Cryptonet Key

COMPUSEC—Computer Security

COMSEC—Communications Security

COPS—Computer Oracle Password and Security

COR—Central Office of Record (COMSEC)

CPI—Critical Program Information

CPS—COMSEC Parent Switch

CRC—Cycle Redundancy Check

CRL—Certificate Revocation List

CRP—COMSEC Resources Program

Crypt/Crypto—Cryptographic-Related

CSE—Communications Security Element

CSET—Computer Security Engineering Team

CSO—Communications and Information Systems Officer

CSS—1. COMSEC Subordinate Switch
2. Constant Surveillance Service
3. Continuous Signature Service
4. Coded Switch System

CSM—Computer Systems Manager

CSSO—1. Computer Systems Security Officer
2. Contractor Special Security Officer

CSTVRP—Computer Security Technical Vulnerability Reporting Program

CTAK—Cipher Text Auto-Key

CT&E—Certification Test and Evaluation

CTTA—Certified Tempest Technical Authority

CVC—Consonant-Vowel-Consonant

CUP—Communications Security Utility Program

DAA—Designated Approving Authority

DAC—Discretionary Access Control

DAMA—Demand Assigned Multiple Access

DES—Data Encryption Standard

DGSA—Defense Goal Security Architecture

DIAP—Defense-Wide Information Assurance Program

DITSCAP—DoD Information Technology Security Certification and Accreditation Process

DoD TCSEC—Department of Defense Trusted Computer System Evaluation Criteria

DLED—Dedicated Loop Encryption Device

DMA—Direct Memory Access

DPL—Degausser Products List (a section in the *Information Systems Security Products and Services Catalogue*)

DSA—Digital Signature Algorithm

DSN—Defense Switched Network

DSVT—Digital Subscriber Voice Terminal

DTLS—Descriptive Top-Level Specification

DTD—Data Transfer Device

DTS—Defense Travel System

DUA—Directory User Agent

EAM—Emergency Action Message

ECCM—Electronic Counter-Countermeasures

ECM—Electronic Countermeasures

ECPL—Endorsed Cryptographic Products List (a section in the *Information Systems Security Products and Services Catalogue*)

EDESPL—Endorsed Data Encryption Standard Products List

EFD—Electronic Fill Device

EFTO—Encrypt For Transmission Only

EGADS—Electronic Generation, Accounting, and Distribution System

EKDD—Electronic Key Distribution Device

EKMS—Electronic Key Management System

ELINT—Electronic Intelligence

ELSEC—Electronic Security

EMSEC—Emission Security

EPL—Evaluated Products List (a section in the *Information Systems Security Products and Services Catalogue*)

ERTZ—Equipment Radiation Tempest Zone

ESA—Emission Security Assessment

ETL—Endorsed Tools List

ETPL—Endorsed Tempest Products List Item

EUCI—Endorsed For Unclassified Cryptographic Information

FCA—Functional Configuration Audit

FDDI—Fiber Distributed Data Interface

FDIU—Fill Device Interface Unit

FIPS—Federal Information Processing Standard

FOCI—Foreign Owned, Controlled, or Influenced

FOUO—For Official Use Only

FSRS—Functional Security Requirements Specification

FSTS—Federal Secure Telephone Service

FTAM—File Transfer Access Management

FTS—Federal Telecommunications System

FW&A—Fraud, Waste, and Abuse

HAG—High Assurance Guard

HUSK—Hardened Unique Storage Key

I&A—Identification and Authentication

IBAC—Identity Based Access Control

IDS—Intrusion Detection System

IDT—Intrusion Detection Tools

IEMATS—Improved Emergency Message Automatic Transmission System

IFFN—Identification, Friend, Foe, or Neutral

IIRK—Interarea Interswitch Rekeying Key

INE—In-Line Network Encryptor

INFOSEC—Information Systems Security

IPAP—Information Protection Assessment Program

IPAT—Information Protection Assessment and Assistance Team

IPM—Interpersonal Messaging

IPSO—Internet Protocol Security Option

IRID—Incident Report Identification

IRK—Interswitch Rekeying Key

ISSM—Information System Security Manager

ISSO—Information System Security Officer

IV&V—Independent Validation and Verification

IW—Information Warfare

IWS—Information Warfare Squadron

KAK—Key-Auto-Key

KDC—Key Distribution Center

KEK—Key Encryption Key

KG—Key Generator

KMC—Key Management Center

KMID—Key Management Identification Number

KMODC—Key Management Ordering and Distribution Center

KMP—Key Management Protocol

KMS—Key Management System

KMSA—Key Management System Agent

KMUA—Key Management User Agent

KP—Key Processor

KPK—Key Production Key

KSD—Key Storage Device

KSOS—Kernelized Secure Operating System

KVG—Key Variable Generator

LEAD—Low-Cost Encryption/Authentication Device

LEAF—Law Enforcement Access Field

LKG—Loop Key Generator

LMD—Local Management Device

LMD/KP—Local Management Device/Key Processor

LME—Layer Management Entry

LMI—Layer Management Interface

LPD—Low Probability Of Detection

LPI—Low Probability Of Intercept

LRIP—Limited Rate Initial Preproduction

LSI—Large Scale Integration

MAC—1. Mandatory Access Control
2. Message Authentication Code

MAN—Mandatory Modification

MCCB—Modification/Configuration Control Board

MD5—Message Digest 5

MDC—Manipulation Detection Code

MEECN—Minimum Essential Emergency Communications Network

MER—Minimum Essential Requirements

MI—Message Indicator

MIJI—Meaconing, Intrusion, Jamming and interference

MISSI—Multilevel information System Security Initiative

MLS—Multilevel Security

MRK—Manual Remote Rekeying

NAC—National Agency Check

NACAM—National COMSEC Advisory Memorandum

NACSI—National COMSEC Instruction

NACSIM—National COMSEC Information Memorandum

NAK—Negative Acknowledge

NCS—1. National Communications System
2. National Cryptologic School
3. Net Control Station

NCSC—National Computer Security Center

NETS—Nationwide Emergency Telecommunications Service

NISAC—National Industrial Security Advisory Committee

NIST—National Institute Of Standards and Technology

NLZ—No-Lone Zone

NSA—National Security Agency

NSAD—Network Security Architecture and Design

NSD—National Security Directive

NSDD—National Security Decision Directive

NSEP—National Security Emergency Preparedness

NSI—National Security Information

NSM—Network Security Monitor

NSO—Network Security Officer

NSTAC—National Security Telecommunications Advisory Committee

NSTISSAM—National Security Telecommunications and Information Systems Security Advisory/ Information Memorandum

NSTISSC— National Security Telecommunications and Information Systems Security Committee

NTCB—Network Trusted Computing Base

NTIA—National Telecommunications and Information Administration

NTISSAM—National Telecommunications and Information Systems Security Advisory/Information Memorandum

OADR—Originating Agency's Determination Required

OLS—On-Line Surveys

OPCODE—Operations Code

OPSEC—Operations Security

ORA—Organizational Registration Authority

OTAD—Over-The-Air key Distribution

OTAR—Over-The-Air Rekeying

OTAT—Over-The-Air key Transfer

OTP—One-Time Pad

OTT—One-Time Tape

PAA—Policy Approving Authority

PAAP—Peer Access Approval

PAE—Peer Access Enforcement

PAL—Permissive Action Link

PCA—Physical Configuration Audit

PCMCIA—Personal Computer Memory Card International Association

PCZProtected Communications Zone

PDR—Preliminary Design Review

PDS—1. Protected Distribution System
2. Practice Dangerous to Security

PDU—Protocol Data Unit

PES—Positive Enable System

PIN—Personal Identification Number

PKA—Public Key Algorithm

PKC—Public Key Cryptography

PKI—Public Key Infrastructure

PKSD—Programmable Key Storage Device

PPL—Preferred Products List (a section in the *Information Systems Security Products and Services Catalogue*)

PRODSEC—Product Security

PROPIN—Proprietary Information

PSL—Protected Services List

PWDS—Protected Wireline Distribution System

QSP—Quick System Profile

RACE—Rapid Automatic Cryptographic Equipment

RAMP—Rating Maintenance Program

RC—Resistive-Capacitive

RQT—Reliability Qualification Tests

SAO—Special Access Office

SAP—Special Access Program

SAR—Special Access Required

SARK—Saville Advanced Remote Keying

SCI—Sensitive Compartmented Information

SDNRIU—Secure Digital Net Radio Interface Unit

SDNS—Secure Data Network System

SFA—Security Fault Analysis

SHA—Secure Hash Algorithm

SHD—Special Handling Designator

SFUG—Security Features Users Guide

SI—Special Intelligence

SIGSEC—Signals Security

SIPRNET—Secret Internet Protocal (IP) Router Network

SMM—Special Mission Mandatory Modification

SMO—Special Mission Optional Modification

SMU—Secure Mobile Unit

SPECAT—Special Category

SPK—Single Point Key(ing)

SPI—Security Profile Inspector

SPS—Scratch Pad Store

SRA—Sub-Registration Authority

SRR—Security Requirements Review

SSO—Special Security Officer

ST&E—Security Test and Evaluation

STS—Subcommittee on Telecommunications Security

TA—Traffic Analysis

TACTED—Tactical Trunk Encryption Device

TAG—Tempest Advisory Group

TAISS—Telecommunications and Automated Information Systems Security

TCB—Trusted Computing Base

TCD—Time Compliance Data

TCP—Transmission Control Protocol

TCSEC—Trusted Computer System Evaluation Criteria

TD—Transfer Device

TED—Trunk Encryption Device

TEK—Traffic Encryption Key

TEP—Tempest Endorsement Program

TFM—Trusted Facility Manual

TFS—Traffic Flow Security

TLS—Top-Level Specification

TNI—Trusted Network Interpretation

TNIEG—Trusted Network Interpretation Environment Guideline

TPC—Two-Person Control

TPDL—Tempest Profile Data List

TPEP—Trusted Products Evaluation Program

TPI—Two-Person Integrity

TRANSEC—Transmission Security

TS—Top Secret

TSCM—Technical Surveillance Countermeasures

TSEC—Telecommunications Security

TSK—Transmission Security Key

UIRK—Unique Interswitch Rekeying Key

UIS—User Interface System

UPP—User Partnership Program

USDE—Undesired Signal Data Emanations

USER-ID—User Identification

VIC—Vulnerability/Incident Control

VIR—Vulnerability and Incident Reports

VST (CFD)—Vinson Subscriber Terminal (Common Fill Device)

VTT (CFD)—Vinson Trunk Terminal (Common Fill Device)

Terms

A1—Highest level of trust defined in the Orange Book (Department of Defense 5200.28-STD, *Trusted Computer System Evaluation Criteria)*.

Administrative Security—Management constraints and supplemental administrative controls established to provide an acceptable level of protection for data. Synonymous with Procedural Security.

Access—1. A user's ability to communicate with (input to or receive output from) a system or to have entry to a specified area. 2. Allowing individuals to review or receive copies of their records.

Access Control List (ACL)—Mechanism implementing discretionary and/or mandatory access control between subjects and objects.

Access Control Mechanism—Security safeguard designed to detect and deny unauthorized access and permit authorized access in an information system.

Access Level—Hierarchical portion of the security level used to identify the sensitivity of information system data and the clearance or authorization of users. Access level, in conjunction with the non-hierarchical categories, forms the sensitivity label of an object. See Category.

Accessible Space—Area within which the user is aware of all persons entering and leaving. This area denies the opportunity for concealed TEMPEST surveillance, and delineates the closest point of potential TEMPEST intercept from a vehicle. Preferred term: Inspectable Space.

Accountability—In communications security, the principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Accounting Legend Code—Numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.

Accreditation—Formal declaration by a designated approving authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. The DAA provides written approval for the operation of each system or network before it can begin processing in a specified facility.

Accreditation Control Number (ACN)—Information concerning the status of a particular AIS accreditation that is entered into the Information Processing Management System (IPMS). The nine position number is composed as follows: first position-highest classification of the system (i.e., T for Top Secret, S for Secret, C for Confidential, U for Unclassified or Sensitive but Unclassified); the next four characters indicate the month and year of accreditation (e.g., 1095 indicates Oct 95); the next character indicates the mode of processing (i.e., D for dedicated, S for system high, M for multilevel, P for partitioned); the next character indicates the level of trust (i.e., A1, B3, B2, B1, C2); and the last character indicates the type of accreditation (i.e., I for interim, and F for final).

Administrative Vulnerability—An AIS security weakness resulting from incorrect or inadequate security safeguards and controls attributable to the system administrator (SA), CSSO, or user. The administrative vulnerability is under the full control of the SA, CSSO or users.

Aggregation—Collection or grouping of independent information where the sensitivity of the whole is greater than the sensitivity of the parts.

Approval to Operate—Concurrence by the designated approving authority that minimum security requirements are met and there is an acceptable level of risk. Accreditation authorizes the operation of a computer system or network at a specific site. See Accreditation and Interim Approval.

Assembly—Group of parts, elements, subassemblies, or circuits that are removable items of communications security equipment.

Attack—Intentional act of attempting to bypass one or more of the following security controls of an Information System: nonrepudiation, authentication, integrity, availability, or confidentiality.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Trail—Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an Information System, to message routing in a communications system, or to the transfer of communications security material.

Authenticate—To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an Information System, or to establish the validity of a transmission.

Authenticator—1. Means used to confirm the identity of a station, originator, or individual. 2. A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission.

Authorization—Access privileges granted to a user, program, or process.

Authorized Vendor Program—A program in which a vendor, producing an Information Systems Security product under contract to the National Security Agency, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors. Products approved for marketing and sale through the Authorized Vendor Program are placed on the Endorsed Cryptographic Products List.

Authorizing Official—The official who authorizes individuals to perform communications security responsibilities at the wing level, the staff directorate (two-letter personnel under the commander) is the authorizing official. At the group level and below, the commander is the authorizing official.

Auto-Manual System—Programmable, hand-held crypto-equipment used to perform encoding and decoding functions.

Automated Information Systems Security—See Information Systems Security.

Automated Security Monitoring—Use of automated procedures to ensure that security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.

Automatic Remote Rekeying—Procedure to rekey a distant crypto-equipment electronically without specific actions by the receiving terminal operator.

Banner—A display on an information system that sets parameters for system or data use.

Bell-La Padula Security Model—Formal-state transition model of a computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations.

Benign—Condition of cryptographic data that cannot be compromised by human access.

Benign Environment—Non-hostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.

Beyond A1—Level of trust defined by the DoD Trusted Computer System Evaluation Criteria to be beyond the state-of-the-art technology. It includes all the Al-level features plus additional ones not required at the Al-level.

Binding—Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.

Biometrics—Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.

Black—Designation applied to communications and information systems, and to associated areas, circuits, components, and equipment, in which national security information is not processed.

Black Key—Encrypted key. See Red Key.

Black Line—Any transmission line in which only unclassified or enciphered signals are carried.

Black Signal—Any signal (e.g., enciphered signal or control signal) that would not divulge national security information if recovered and analyzed.

Boundary—Software, hardware, or physical barrier that limits access to a system or part of a system.

Breach—The successful defeat of security controls, which, if carried to consummation, could result in a penetration of an AIS.

Brevity List—List containing words and phrases used to shorten messages.

Bulk Encryption Simultaneous encryption of all channels of a multichannel telecommunications link.

Call Back—Procedure for identifying and authenticating a remote communications and information system terminal, whereby the host system disconnects the terminal and re-establishes contact. Synonymous with Dial Back.

Call Sign Cipher (CFD)—Cryptosystem used to encipher/decipher call signs, address groups, and address indicating groups.

Canister—Type of protective package used to contain and dispense key in punched or printed tape form.

Capability—Protected identifier that both identifies the object and specifies the access rights to be allowed to the subject who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be subject possesses a capability for the object.

Cascading—Downward flow of information through a range of security levels greater than the accreditation range of a system network or component.

Category—1. Restrictive label applied to classified or unclassified information to limit access. 2. A grouping of classified or SBU information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., Formal Access Approval). Examples include proprietary, For Official Use Only (FOUO), Privacy Act, NATO, and compartmented information.

Controlled Access Protection (CAP) Administrator—Individual responsible for granting and withdrawing cryptographic access within a unit or organization.

Controlled Cryptographic Item (CCI) Assembly—Device embodying a cryptographic logic or other communications security design that NSA has approved as a Controlled Cryptographic Item. It performs the entire communications security function, but depends upon the host equipment to operate.

Controlled Cryptographic Item (CCI) Component—Part of a Controlled Cryptographic Item that does not perform the entire communications security function but depends upon the host equipment, or assembly, to complete and operate the communications security function.

Controlled Cryptographic Item (CCI) Equipment—Telecommunications or information handling equipment that embodies a Controlled Cryptographic Item component or assembly and performs the entire communications security function without dependence on host equipment to operate.

Central Office Of Record (COR)—Office of a federal department or agency that keeps records of accountable communications security material held by elements subject to its oversight.

Certificate—Record holding security information about an communications and information system user and vouches to the truth and accuracy of the information it contains.

Certificate of Action Statement—A statement attached to a communications security audit report by which a communications security custodian certifies that all actions have been completed.

Certificate Management—Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.

Certificate Revocation List—List of invalid certificates (as defined above) that have been revoked by the issuer.

Certification—Comprehensive evaluation of the technical and nontechnical security features of an automated information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Agent—Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Certification Authority (CA)—Third level Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by the parent Policy Creation Authority (PCA).

Certification Authority Workstation (CAW)—A commercial off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates.

Certification Level—A measure of the level-of-effort required to certify and accredit an information system. It identifies the required certification steps and the minimum documentation, tests, and reports. The certification level is calculated using the degrees of assurance.

Certification Package—Product of the certification effort documenting the detailed results of the certification activities.

Certification Test And Evaluation (CT&E)—Software and hardware security tests conducted during development of an Information System.

Certified Tempest Technical Authority (CTTA)—An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

Certifying Official—Individual responsible for making a technical judgment of the automated information system's compliance with stated security requirements and requesting approval to operate from the designated approval authority.

Challenge And Reply Authentication—Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.

Checksum—Value computed on data to detect error or manipulation during transmission. See Hash Total.

Check Word—Cipher text generated by cryptographic logic to detect failures in cryptography.

Cipher—Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text or in which units of plain text are rearranged, or both.

Cipher Text—Enciphered information.

Cipher Text Auto-Key—Cryptographic logic which uses previous cipher text to generate a key stream.

Ciphony—Process of enciphering audio information, resulting in encrypted speech.

Classified Information—1. Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the *Atomic Energy Act of 1954*, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. 2. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

Classified Cryptographic Information—Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, including depot-level maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic computer software.

Clearance—An individual's level of access to classified information. The official determination of a person's trustworthiness, based on a records review and past behavior.

Clearing—Removal of data from a communications and information system, its storage devices and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing.

Closed Security Environment—Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control**.**

Code—1. System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. 2. A cryptosystem in which the cryptographic equivalents (usually called "code groups") typically consisting of letters or digits (or both) in otherwise meaningless combinations are substituted for plain text elements which are primarily words, phrases, or sentences. See also cryptosystem.

Code Book—In communications security, a book or other document containing plain text and its code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.

Code Group—In communications security, a group of letters, numbers, or both, in a code system used to represent a plain text word, phrase, or sentence.

Code Vocabulary—Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.

Coercivity—Amount of applied magnetic field (of opposite polarity) required to reduce magnetic induction to zero. Coercivity is measured in oersteds (Oe). It is often used to represent the relative difficulty of degaussing various magnetic media.

Cognizant Security Authority (CSA)—An individual, usually at the MAJCOM level, who is authorized to make communications security policy decisions based on current Air Force communications security doctrine.

Cold Start—Procedure for initially keying crypto-equipment.

Collateral Information—All national security information classified under the provisions of an executive order, for which special community systems of compartments (e.g., sensitive compartmented information) are not formally established.

Command Authority—Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Communications and Information Systems Security—The protection afforded to communications and information systems to preserve the availability, integrity, and confidentiality of the systems and the information contained within the systems. Such protection is the integrated application of communications security, TEMPEST, and COMPUSEC.

Commercial communications security (COMSEC) Endorsement Program (CCEP)—Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the CCEP may include modules, subsystems, equipment, systems, and ancillary devices.

Common Fill Device—One of a family of devices developed to read-in, transfer, or store key.

Communications Cover—Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.

Communications Deception—Use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system.

Communications Profile—Analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.

Communications Security (COMSEC)—1. Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material. 2. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

Communications Security (COMSEC) Account—Administrative entity, identified by an account number, used to maintain accountability, custody, and control of communications security material.

Communications Security (COMSEC) Aid—COMSEC material that assists in securing telecommunications and is required in the production, operation, or maintenance of COMSEC systems and their components. COMSEC keying material, call sign/ frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.

Communications Security (COMSEC) Boundary—Definable perimeter that encompasses all hardware, firmware, and software components performing critical COMSEC functions, such as key generation and key handling and storage.

Communications Security (COMSEC) Chip Set—A collection of National Security Agency approved microchips.

Communications Security (COMSEC) Control Program—Computer instructions or routines that controlling or affect the externally performed functions of key generation, key distribution, message encryption and decryption, or authentication.

Communications Security (COMSEC) Custodian—Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account.

Communications Security (COMSEC) End Item—A final combination of equipment or component parts ready for its intended use in a COMSEC application.

Communications Security (COMSEC) Equipment—Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto ancillary equipment, crypto production equipment, and authentication equipment.

Communications Security (COMSEC) Facility—Physical space used for generating, storing, repairing, or using COMSEC material.

Communications Security (COMSEC) Incident—See Incident.

Communications Security (COMSEC) Incident Monitoring Activity—The office within an Air Force organization that maintains a record of COMSEC activity incidents caused by elements of that organization and makes sure all actions required in connection with the incident are completed.

Communications Security (COMSEC) Insecurity—COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

Communications Security (COMSEC) Material—Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to: key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

Communications Security (COMSEC) Material Control System (CMCS)—Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, crypto logistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the COMSEC Material Control System.

Communications Security (COMSEC) Modification—See Information Systems Security Equipment Modification.

Communications Security (COMSEC) Module—Removable component that performs COMSEC functions in a telecommunications equipment or system.

Communications Security (COMSEC) Monitoring—Act of listening to, copying, or recording transmission of one's own official telecommunications to analyze the degree of security.

Communications Security (COMSEC) No-Lone Zone—Area, room, or space that, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other.

Communications Security (COMSEC) Operations—COMSEC operations include distributing, safeguarding, destroying, and accounting for all COMSEC material at all administrative and operational COMSEC accounts and all COMSEC user locations.

Communications Security (COMSEC) Profile—Statement of COMSEC measures and materials used to protect a given operation, system, or organization.

Communications Security (COMSEC) Responsible Officer (CRO)— Individual authorized by an organization to order COMSEC aids from the COMSEC account and who is responsible for their protection.

Communications Security (COMSEC) Survey—Organized collection of COMSEC and communications information relative to a given operation, system, or organization.

Communications Security (COMSEC) System Data—Information required by a COMSEC equipment or system to enable it to properly handle and control key.

Communications Security (COMSEC) Training—Teaching of skills relating to COMSEC accounting, use of COMSEC aids, or installation, use, maintenance, and repair of COMSEC equipment.

Compartmentalization—A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone. Compartmented information is usually identified by a codeword and level of classification.

Compartmented Mode—Information systems security mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (a) Valid security clearance for the most restricted information processed in the system. (b) Formal access approval and signed non-disclosure agreements for that information to which a user is to have access. (c) Valid need-to-know for information to which a user is to have access.

Compromise—Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Compromising Emanations—Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by communications and information system equipment. See TEMPEST.

Computer Abuse—Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources.

Computer-Based Security—Security for the communications and information system provided through the use of automated security features.

Computer Crime—Fraud, embezzlement, unauthorized access, and other crimes committed with the aid of or directly involving an automated information system.

Computer Cryptography—Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.

Computer Intrusion—An event of unauthorized entry, or attempted entry, to a computer system.

Computer Security (COMPUSEC)—The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.

Computer Security Engineering Team (CSET)—Deployable Air Force Information Warfare Center teams that provide assistance to computer users and to Air Force organizations. The teams also provide assistance to control and recover from intrusion activity.

Computer Security Incident—See Incident.

Computer Security Policy—Set of laws, rules, and practices that regulate how an organization protects computer systems and the data within them.

Computer System Security Officer (CSSO)—Official who manages the COMPUSEC program for an AIS assigned to them by the CSM; including monitoring AIS activities, and ensuring that the AIS is operated, maintained, and disposed of according to security policies and practices.

Computer Security Subsystem—Hardware/software designed to provide computer security features in a larger system environment.

Computer Security Technical Vulnerability Reporting Program (CSTVRP)—Program that focuses on technical vulnerabilities in commercially available hardware, firmware, and software products acquired by DoD. **NOTE**: CSTVRP provides for reporting, cataloging, and discreet dissemination of technical vulnerability and corrective-measure information on a need-to-know basis.

Confidentiality—Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Control—Process of controlling modifications to hardware, firmware, software, and documentation to ensure the communications and information system is protected against improper modifications.

Configuration Management—Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the life cycle of an communications and information system.

Confinement Property—Synonymous with Property.

Contamination—1. The introduction of data of one security classification or security category into data of a lower security classification or different security category. 2**.** Intermixing of data at different sensitivity and need-to-know levels. The lower level data is said to be contaminated by the higher level data; thus, the contaminating (higher level) data may not receive the required level of protection.

Contingency Key—Key held for use under specific operational conditions or in support of specific contingency plans.

Control—In communications security, prescribed actions taken to maintain the appropriate level-of-protection for communications and information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of communications and information system activities, or report incidents.

Controlled Access Protection—The C2 level of protection described in the Trusted Computer System Evaluation Criteria (Orange Book). Its major characteristics are: individual accountability, audit, access control, and object reuse.

Controlled Area—In communications security, any building, area, or structure containing Air Force resources that are a lucrative target for theft, compromise, or destruction and to which entry must be limited to provide more protection.

Controlled Cryptographic Item (CCI) Assembly—Device embodying a cryptographic logic or other COMSEC design that the National Security Agency has approved as a CCI and performs the entire COMSEC function, but is dependent upon the host equipment to operate.

Controlled Cryptographic Item (CCI) Component—Device embodying a cryptographic logic or other COMSEC design, that the National Security Agency has approved as a CCI, that does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete and operate the COMSEC function.

Controlled Cryptographic Item (CCI)—Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI."

Controlled Sharing—Condition that exists when access control is applied to all users and components of an information system.

Controlled Space—Three-dimensional space surrounding communications and information system equipment, within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance.

Controlling Authority—Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.

Cooperative Key Generation (CKG)—Electronically exchanged functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.

Correctness Proof—A mathematical proof of consistency between a specification and its implementation.

Cost-Benefit Analysis—Assessment of the cost of providing protection or security commensurate with the risk and magnitude of asset loss or damage.

Countermeasure (CM)—1. Any action, device, procedure, technique, or other measure that reduces the vulnerability of an Information System; also called a safeguard. A countermeasure protects against a specific threat type or mechanism. 2**.** The sum of a safeguard and its associated controls.

Countermeasures Review—A technical evaluation of a facility to identify the inspectable space, the required countermeasures, and the most cost effective way to apply required countermeasures.

Covert Channel—Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an communications and information system security policy. See Overt Channel and Exploitable Channel.

Covert Channel Analysi—Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.

Covert Storage Channel—Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel—Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.

Cracker—A person who attempts to gain access to computers for which he or she does not have authorization.

Credentials—Information, passed from one entity to another, that is used to establish the sending entity's access rights.

Criticality—Computer security characteristic that measures how important the correct and uninterrupted functioning of the communications and information system is to national security, human life or safety, or the mission of the using organization.

Critical Processing—Processing that must continue in a correct and uninterrupted manner to support DoD emergency or war plans, preserve human life or safety, or support the mission of the using organization.

Critical Program Information—Technologies, programs, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

Cryptanalysis—Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Crypto—Marking or designator identifying communications security keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information.

Crypto-Alarm—Circuit or device that detects failures or aberrations in the logic or operation of crypto-equipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm.

Crypto-Algorithm—Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc.

Crypto-Ancillary Equipment—Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, without performing cryptographic functions itself.

Crypto-Channel—A complete system of crypto-communications between two or more holders. The basic unit for naval cryptographic communication. It includes: (a) the cryptographic aids prescribed; (b) the holders thereof; (c) the indicators or other means of identification; (d) the area or areas in which effective; (e) the special purpose, if any, for which provided; and (f) pertinent notes as to distribution, usage, etc. A crypto-channel is analogous to a radio circuit.

Crypto-Equipment—Equipment that embodies a cryptographic logic.

Cryptographic Access Program (CAP)—A program to protect national security information and to govern access to cryptographic information that the DoD produces, controls, or owns.

Cryptographic Component—Hardware or firmware embodiment of the cryptographic logic. Cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items.

Cryptographic Equipment Room (CER)—Controlled-access room in which cryptosystems are located**.**

Cryptographic Information—All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial**.**

Cryptographic Initialization—Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode**.**

Cryptographic Logic—The embodiment of one or more crypto-algorithms along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process.

Cryptographic Randomization—Function that randomly determines the transmit state of a cryptographic logic**.**

Cryptography—Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form**.**

Crypto-Ignition Key (CIK)—Device or electronic key used to unlock the secure mode of crypto-equipment.

Cryptomaterial—All material, including documents, devices, equipment, and apparatus, essential to the encryption, decryption, or authentication of telecommunications. When classified, it is designated CRYPTO and subject to special safeguards.

Cryptonet—Stations holding a common key**.**

Crytonet Member—An individual station, among a group of stations, holding a specific key for use. Controlling authorities are defacto cryptonet members.

Cryptopart—A division of a message as prescribed for security reasons. The operating instructions for certain crypto systems prescribe the number of groups which may be encrypted in the systems, using a single message indicator. Crypto parts are identified in plain language. They are not to be confused with message parts.

Cryptoperiod—Time span during which each key setting remains in effect.

Cryptosecurity—Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

Cryptosynchronization—Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.

Cryptosystem—Associated information systems security items interacting to provide a single means of encryption or decryption.

Cryptosystem Assessment—Process of establishing the exploitability of a cryptosystem, normally by reviewing transmitted traffic protected or secured by the system under study.

Cryptosystem Evaluation—Process of determining vulnerabilities of a cryptosystem.

Cryptosystem Review—Examination of a cryptosystem by the controlling authority to ensure its adequacy of design and content, continued need, and proper distribution**.**

Cryptosystem Survey—Management technique in which actual holders of a cryptosystem express opinions on the system's suitability and provide usage information for technical evaluations.

Cyclic Redundancy Check—Error checking mechanism that checks data integrity by computing a polynomial algorithm based checksum.

Dangling Threat—Set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk.

Dangling Vulnerability—Set of properties about the internal environment for which there is no corresponding threat and therefore no implied risk.

Data Aggregation—1. The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified. 2. Data aggregation is the convergence of information. This becomes a problem when certain information or data elements at one sensitivity level requires reclassification at a higher level when combined or associated with other information. Aggregate data would require classification if the new information meets the specific classifying criteria as defined in DoD 5200.1-R or reclassification according to classification guidance provided by the functional OPR.

Data Contamination—Deliberate or accidental process or act resulting in a change in the integrity of the original data. See Data Diddling.

Data Diddling—Process of accidentally or maliciously changing data before or during the input or output to a computer. The changes can be made by anyone associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, or transforming the data. See Data Contamination.

Data Encryption Standard (DES)—Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology in Federal Information Processing Standard 46-2, *Data Encryption Standard*.

Data Flow Control—Synonymous with information flow control.

Data Integrity— 1. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. 2. The attribute of data relating to the preservation of its meaning and completeness; the consistency of its representations; and its correspondence to what it represents.

Data Origin Authentication—Corroboration that the source of data is as claimed**.**

Data Security—Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Data Sensitivity—The identification of how important the data processed by the system is and the extent of the protection that must therefore be provided to the system and its data.

Data Transfer Device (DTD)—Fill device designed to securely store, transport, and transfer electronically both communications security and transmission security key, designed to be backwards compatible with the previous generation of communications security common fill devices, and programmable to support modern mission systems.

Decertification—Revocation of the certification of an information system item or equipment for cause**.**

Decipher—Convert enciphered text to plain text by means of a cryptographic system.

Declassification—The determination that in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation.

Declassification (Of Magnetic Storage Media)—Administrative decision or procedure to remove or reduce the security classification of the subject media.

Declassify—To cancel the security classification of an item of classified matter. See also downgrade**.**

Decode—Convert encoded text to plain text by means of a code.

Decrypt—1. Generic term encompassing decode and decipher. 2. To convert encrypted text into its equivalent plain text by means of a cryptosystem. (This does not include solution by crypto-analysis.) **NOTE**: The term Decrypt covers the meanings of Decipher and Decode. See also Cryptosystem.

Dedicated Mode—Information system security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) Valid security clearance for all information within the system. (b) Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs). (c) Valid need-to-know for all information contained within the Information System. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Default Classification—Temporary classification reflecting the highest classification being processed in an Information System. Default classification is included in the caution statement affixed to an object.

Defense-Wide Information Assurance Program (DIAP)—An overarching DoD-level program established by the Deputy Secretary of Defense to ensure the protection and reliability of the Defense Information Infrastructure. The DIAP implements a DoD-wide Information Assurance planning and integration framework. It infuses Information Assurance throughout DoD operations as a fundamental element of readiness and training.

Degausser—Electrical device or hand held permanent magnet that can generate a high intensive magnetic field to purge magnetic storage media.

Degausser Products List (DPL)—List of commercially produced degaussers that meet National Security Agency specifications. This list is included in the National Security Agency Information Systems Security Products and Services Catalogue, and is available through the Government Printing Office.

Degrees Of Assurance—Measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. The degrees of assurance (i.e., low, medium, and high) for availability, integrity, confidentiality, and authenticity are directly related to the expected consequences resulting from loss of systems or information.

Delegated Development Program—Information security program in which the director, National Security Agency, delegates, on a case by case basis, the development and/or production of an entire telecommunications product, including the information systems security portion, to a lead department or agency.

Denial of Service—Result of any action or series of actions that prevents any part of a communications and information system from functioning.

Descriptive Top-Level Specification—Top-level specification written in a natural language (e.g., English), an informal design notation, or a combination of the two. Descriptive top-level specification, required for a class B2 and B3 Information System, completely and accurately describes a trusted computing base. See Formal Top-Level Specification.

Design Controlled Spare Part—Part or subassembly for a communications security item of equipment or device with a National Security Agency controlled design.

Design Documentation—Set of documents, required for Trusted Computer System Evaluation Criteria (TCSEC) classes C1 and above (as defined in the Orange Book, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD), whose primary purpose is to define and describe the properties of a system. As it relates to TCSEC, design documentation provides an explanation of how the security policy of a system is translated into a technical solution via the Trusted Computer Base hardware, software, and firmware.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority, Delegated Accrediting Authority, and Communications And Information Systems Security Manager.

Digital Signature—Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation. Same as Electronic Signature.

Digital Signature Algorithm—Procedure that appends data to, or performs a cryptographic transformation of, a data unit. The appended data or cryptographic transformation allows reception of the data unit and protects against forgery, e.g., by the recipient.

Discretionary Access Control (DAC)—Means of restricting access to objects based on the identity and need- to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

Discretionary Protection—Access control features that identify individual users and their need-to-know and limits them to certain, specified information. See Discretionary Access Control.

Discretionary Security Protection—Trusted computing base that provides elementary discretionary access control protection (Class C1) features that separate users from data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis (i.e., suitable for allowing users to be able to protect private data and to keep other users from accidentally reading or destroying that data).

DoD Trusted Computer System Evaluation Criteria (TCSEC)—Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into an Information System. This document, DoD 5200.28 STD, is commonly referred to as the Orange Book.

Dominate—Term used to compare communications and information system security levels. Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than, or equal to, that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.

Drop Accountability—Procedure under which a communications security (COMSEC) account custodian initially receipts for COMSEC material, and then provides no further accounting for it to its central office of record. Local accountability of the COMSEC material may continue to be required. See Accounting Legend Code.

Economic Assessment—Comparison of the benefits of proposed security measures versus their cost. An economic assessment aids in planning and selecting security measures.

Electronically Generated Key—Key generated in a communications security device by introducing (either mechanically or electronically) a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key.

Electronic Key Management System (EKMS)—Interoperable collection of systems being developed services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of communications security material.

Electronic Messaging Services—Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yield a business-quality electronic mail service suitable for the conduct of official government business.

Electronic Security—Protection resulting from measures designed to deny unauthorized persons information derived from the interception and analysis of noncommunications electromagnetic radiations.

Electronic Signature—Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Same as Digital Signature.

Electronic Security Assessment—One of three levels of capability to improve communications-computer systems security posture by accurately measuring the posture and recommending countermeasures where deficiencies exist.

Element—Removable item of communications security equipment, assembly, or subassembly that normally consists of a single piece or group of replaceable parts.

Emanation—Unintended signals or noise appearing external to an equipment.

Embedded Cryptography—Cryptography engineered into an equipment or system whose basic function is not cryptographic.

Embedded Cryptographic System—Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem.

Emission Control—The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: (a) detection by enemy sensors; (b) minimize mutual interference among friendly systems; and/or (c) execute a military deception plan.

Emission Security—Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system.

Emission Security (EMSEC) Assessment—An evaluation of a facility to determine the need for emission security.

Encipher—Convert plain text to cipher text by means of a cryptographic system.

Encode—Convert plain text to cipher text by means of a code.

Encrypt—Generic term encompassing encipher and encode.

Endorsed DES Equipment—Unclassified equipment that embodies unclassified data encryption standard cryptographic logic and has been endorsed by the National Security Agency for the protection of national security information.

Encryption Algorithm—Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

End-Item Accounting—Accounting for all the accountable components of communications security equipment configuration by a single short title.

Endorsed for Unclassified Cryptographic Item—Unclassified cryptographic equipment that embodies a U.S. Government classified cryptographic logic and is endorsed by the National Security Agency for the protection of national security information. See Type 2 product.

Endorsement—National Security Agency approval of a commercially-developed product for safeguarding national security information.

End-To-End Encryption—Encryption of information at its origin and decryption at its intended destination without intermediate decryption.

End-To-End Security—Safeguarding information in an information system from point of origin to point of destination.

Entrapment—Deliberate planting of apparent flaws in an communications and information system for the purpose of detecting attempted penetrations.

Equipment Radiation Tempest Zone (ERTZ)—A zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

Erasure—Process intended to render magnetically stored information irretrievable by normal means.

Evaluated Products List (EPL)—Equipment, hardware, software, and/or firmware evaluated by the NCSC in accordance with DoD TCSEC and found to be technically compliant at a particular level of trust. The EPL is the National Security Agency Information Systems Security Products and Services Catalogue.

Executive State—One of several states in which an communications and information system may operate, and the only one in which certain privileged instructions may be executed. Such privileged instructions cannot be executed when the system is operating in other (e.g., user) states. Synonymous with Supervisor State.

Exercise Key—Key used exclusively to safeguard communications transmitted over-the-air during military or organized civil training exercises.

Expired Password—Password that must be changed by the user, or other authorized individual, before log in may be completed.

Exploitable Channel—Channel that allows the violation of the security policy governing an communications and information system and is usable or detectable by subjects external to the trusted computing base. See Covert Channel.

Extraction Resistance—Capability of crypto-equipment or secure telecommunications equipment to resist efforts to extract key.

Fail Safe—Automatic protection of programs and/or processing systems when hardware or software failure is detected.

Fail Soft—Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.

Failure Access—Unauthorized access to data resulting from hardware or software failure.

Failure Control—Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.

Fetch Protection—Communications and information system hardware provided restriction to prevent a program from accessing data in another user's segment of storage.

File Protection—Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.

File Security—Means by which access to computer files is limited to authorized users only.

Fill Device—Communications security item used to transfer or store key in electronic form or to insert key into a crypto-equipment.

Firefly—Key management protocol based on public key cryptography.

Firewall—Gateway, bridge, router, or front-end processor that limits access between networks in accordance with local security policy. Synonymous with front-end security filters.

Firmware—Program recorded in permanent or semi-permanent computer memory.

Fixed Communications Security (COMSEC) Facility—COMSEC facility located in an immobile structure or aboard a ship.

Flash—A specific family of EEPROM devices that hold their content without power. It can be erased in fixed blocks rather than single bytes. Block sizes range from 512 bytes up to 256 kbps.

Flaw—Error of commission, omission, or oversight in an communications and information system that may allow protection mechanisms to be by-passed.

Flaw Hypothesis Methodology—System analysis and penetration technique in which the specification and documentation for an communications and information system are analyzed to produce a list of hypothetical flaws. This list is prioritized on the basis of the estimated probability that a flaw exists on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.

Formal Access Approval—Documented approval by a data owner to allow access to a particular category of information.

Formal Cryptographic Access (FCA)—Formal approval permitting access to COMSEC keying material and prior consent to a non-lifestyle, counterintelligence-scope polygraph examination.

Formal Development Methodology—Software development strategy that proves security design specifications.

Formal Proof—Complete and convincing mathematical argument presenting the full logical justification for each proof step and for the truth of a theorem or set of theorems. These formal proofs provide A1 and beyond A1 assurance under the DoD Trusted Computer System Evaluation Criteria (Orange Book).

Formal Security Policy Model—Mathematically precise statement of a security policy. Such a model must define a secure state, an initial state, and how the model represents changes in state. The model must be shown to be secure by proving that the initial state is secure and that all possible subsequent states remain secure.

Formal Top-Level Specification—Top-level specification written in a formal mathematical language to allow theorems, showing the correspondence of the system specification to its formal requirements, to be hypothesized and formally proven.

Formal Verification—Process of using formal proofs to demonstrate the consistency between formal specification of a system and formal security policy model (design verification) or between formal specification and its high-level program implementation (implementation verification).

Front-End Security Filter—Security filter logically separated from the remainder of an communications and information system to protect system integrity. Synonymous with Firewall.

Functional Office Of Primary Responsibility (OPR)—Organization (e.g. division, directorate, or unit) that employs, but may not own, AISs to perform its mission (function). **NOTE**: Normally they own the data that is stored or processed on the AIS.

Fundamental Requirements—Six fundamental security requirements that deal with controlling access to information are: security policy; marking; identification; accountability; assurance; and continuous protection.

Hardware Security—Equipment features or devices used in a computer system to preclude unauthorized data access or support a trusted computing base.

Hardwired Key—Permanently installed key.

Hazard—A measure of both the existence and the compromising nature of an emanation. Hazards exist if and only if compromising emanations are detectable beyond the inspectable space.

High Risk Environment—Specific location or geographic area where there are insufficient friendly security forces to ensure the safeguarding of communications and information system security equipment.

High Threat Environment—See High Risk Environment.

Identity Token—1. Smart card, metal key, or other physical object used to authenticate identity. 2. Smart card, metal key, or some other physical token carried by a system's user allowing user identity validation.

Identity Validation—Tests enabling an communications and information system to authenticate users or resources.

Imitative Communications Deception—Introduction of deceptive messages or signals into an adversary's telecommunications signals. See Communications Deception and Manipulative Communications Deception.

Impersonating—Form of spoofing.

Implant—Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations.

Inadvertent Disclosure—Accidental exposure of information to a person not authorized access.

Inadvertent Exposure—The accidental disclosure of COMSEC information to a person who does not have authorized access.

Incident—Unauthorized access or entry (or attempt) to an AIS. It can include browsing; disruption or denial of service; alteration or destruction of input, processing, storage, or output of information; or changes to AIS hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

Incomplete Parameter Checking—System flaw that exists when the operating system does not check all parameters fully for accuracy and consistency, thus making the system vulnerable to penetration.

Indicator—An action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

Individual Accountability—Ability to associate positively the identity of a user with the time, method, and degree of access to an information system.

Information Assurance—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities**.**

Information Assurance Red Team (IA)—Information operations (IO) protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Flow Control—Procedure to ensure that information transfers within an communications and information system are not made from a higher security level object to an object of a lower security level.

Information Label—Piece of information that accurately and completely represents the sensitivity of the data in a subject or object. **NOTE:** Information label consists of a security label and other required security markings (e.g., codewords, dissemination control markings, and handling caveats) to be used for data information security labeling purposes. See Label.

Information Protection—Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems.

Information Protection Operations—Proactive security functions established to assist Air Force organizations to deter, detect, isolate, contain, and recover from intrusions of computers and computer networks.

Information Protection Services Effectiveness—One or more absolute qualities that are characterized on a pass or fail basis.

Information Protection Services Efficiency—One or more relative measures that are characterized as a range of quantities subject to continual improvements.

Information Protection Services Interoperability—The ability of two or more systems to exchange data and to mutually use the exchanged data without reformatting.

Information Protection Services Portability—The ability to migrate software and supporting data from one platform to another, with minimum of tailoring. User portability is the ability of users to move from system to system and between different applications on the same system, with minimum of retraining.

Information Protection Services Scalability—The ability to provide functionality up and down a graduated series of application platforms that differ in the speed and capacity, with out loss of functionality.

Information Protection Tools—Tools that perform numerous security functions including boundary protection, viral detection, intrusion detection, profile inspection, network mapping, remote patching, and on-line surveys.

Information Security (INFOSEC)—The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

Information Systems Security (INFOSEC) Equipment Modification—Modification of any fielded hardware, firmware, software, or portion thereof, under National Security Agency configuration control. There are three classes of modification: Mandatory (to include human safety); optional/special mission modifications; and repairs actions. These classes apply to elements, subassemblies, equipment, systems, and software packages performing functions such as key generations, key distribution, messages encryption, decryption, authentication, or those mechanisms necessary to satisfy security policy, labeling, identification, or accountability**.**

Information Systems Security Officer (ISSO)—Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with Systems Security Officer.

Information Systems Security Product—Item (chip, module, assembly, or equipment), technique, product or service that performs or relates to information systems security.

Initialize—Setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

Inspectable Space—Three dimensional space surrounding equipment that process classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists. Synonymous with Zone Control.

Integrity—Quality of an information system that reflects the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Integrity Check Value—Checksum capable of detecting modification of an information system.

Interface—Common boundary between independent systems or modules where interactions take place.

Interface Control Document—Technical document that describes interface controls and identifies the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the information system life cycle.

Interim Approval—Temporary authorization granted by a designated approving authority for an information system to process information based on preliminary results of a security evaluation of the system.

Internetwork Private Line Interface—Network cryptographic unit that provides secure connections, singularly or in simultaneous multiple connections, between a host and a predetermined set of corresponding hosts.

IP Perspective—A philosophy where all security disciplines are coupled together with COMPUSEC to provide complete security for sensitive and classified information. In order to provide realistic and effective security for a system, certification must include all appropriate security disciplines.

Key—Usually a sequence of random or pseudo-random bits used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key.

Key-Auto-Key—Cryptographic logic that uses previous key to produce key.

Key Card (CFD)—Paper card, containing a pattern of punched holes, that establishes key for a specific cryptonet at a specific time.

Key Distribution Center (KDC)—COMSEC facility that generates and distributes key in electrical form.

Key-Encryption-Key (KEK)—Key that encrypts or decrypts other key for transmission or storage.

Key List—Printed series of key settings for a specific cryptonet. Key lists may be produced in list, pad, or printed tape format.

Key Management—Supervision and control of the process whereby key is generated, stored, protected, transferred, loaded, used, and destroyed.

Key Production Key—Key used to initialize a keystream generator for the production of other electronically generated key.

Key Pair—Public key and its corresponding private key as used in public key cryptography.

Key Storage Device (KSD)—A small device, shaped like a physical key which contains passive memory. It is used as a fill device and also as a crypto-ignition key (CIK) for a type I STU-III terminal.

Key Stream—Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.

Key Tag—Identification information associated with certain types of electronic key.

Key Tape—Punched or magnetic tape containing key. Printed key in tape form is referred to as a key list.

Key Updating—Irreversible cryptographic process for modifying key.

Keying Material—Key, code, or authentication information in physical or magnetic form.

Labeled Security Protection (Class B1)—Elementary-level mandatory access control protection features and intermediate-level discretionary access control features in a trusted computing base that use sensitivity labels to make access control decisions.

Least Privilege—Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

Level Of Protection—Extent to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are: (1) Basic: information system and networks requiring implementation of standard minimum security countermeasures. (2) Medium: information system and networks requiring layering of additional safeguards above the standard minimum security countermeasures. (3) High: information system and networks requiring the most stringent protection and rigorous security countermeasures.

Link Encryption—Encryption of information between nodes of a communications system.

List-Oriented—Computer protection in which each protected object has a list of all subjects authorized to access it. See also Ticket-Oriented.

Local Authority—Organization responsible for generating and signing user certificates.

Local Management Device/Key Processor (LMD/KP)—An EKMS platform that provides automated management of COMSEC material and generates key for designated users.

Logic Bomb—A resident computer program that triggers the perpetration of an unauthorized act when particulat states of the system are realized.

Logical Completeness Measure—Means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets security specifications.

Machine Cryptosystem—Cryptosystem in which cryptographic processes are performed by crypto-equipment.

Mandatory Access Control (MAC)—Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need to know) of subjects to access information of such sensitivity. See Discretionary Access Control.

Manual Remote Rekeying—Procedure by which a distant crypto-equipment is rekeyed electrically, with specific actions required by the receiving terminal operator.

Masquerading—Form of spoofing.

Master Crypto-Ignition Key (CIK)—A key device with electronic logic and circuits, providing the capability for adding more operational CIKs to a keyset (maximum of seven) any time after fill procedure is completed. The master CIK can only be made during the fill procedure as the first CIK.

Memory Scavenging—The collection of residual information from data storage.

Message Indicator—Sequence of bits transmitted over a communications system for synchronizing crypto-equipment. Some off-line cryptosystems, such as the KL-51 and one-time pad systems, employ message indicators to establish decryption starting points.

Mimicking—Form of spoofing.

Minimal Protection (Class D)—Class reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation.

Multilevel Device—Equipment trusted to properly maintain and separate data of different security categories.

Multilevel Mode—Information systems security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: (a) Some users do not have a valid security clearance for all the information processed in the Information System. (b) All users have the proper security clearance and appropriate formal access approval for that information to which they have access. (c) All users have a valid need-to-know only for information to which they have access.

Multilevel Security (MLS)—1. Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. 2. Concept of processing information with different classifications and categories that simultaneously permits access to users with different security clearances, but prevents users accessing information for which they lack authorization.

National Security Information—Any information that has been determined pursuant to Executive Order 12356 or any predecessor order to require protection against unauthorized disclosure and is so designated.

Network Mapping (NMAP)—NMAP is information on specific information systems consisting of type of hardware, software loaded in the information systems, operational description, criticality of information systems, accreditation status and date, sensitivity, location, IP address, and systems administrator points of contact.

National Security Telecommunications and Information Systems Security Instruction (NSTISSI)—

A series of documents that establishes the technical criteria for specific national security telecommunications and automated information systems security matters.

Network Security—The protection of networks and their services from destruction, unauthorized modification, or disclosure providing an assurance that the network performs its critical functions correctly and that there are no harmful side-effects.

Network Sponsor—Individual or organization responsible for stating the security policy enforced by the network, for designing the network security architecture to properly enforce that policy, and for ensuring that the network is implemented in such a way that the policy is enforced. For commercial-off-the-shelf systems, the network sponsor will normally be the vendor. For a fielded network system, the sponsor will normally be the project manager or system administrator.

Network System—System implemented with a collection of interconnected components. A network system is based on a coherent security architecture and design.

Network Trusted Computing Base (NTCB)—Totality of protection mechanisms within a network, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. See trusted computing base.

Network Trusted Computing Base (NTCB) Partition—Totality of mechanisms within a single network component for enforcing the network policy, as allocated to that component; the part of the NTCB within a single network component.

Network Weaving—Penetration technique in which different communication networks are linked to access an communications and information system to avoid detection and trace-back.

Non-Discretionary Security—Aspect of DoD security policy that restricts access on the basis of security levels. A security level is composed of a read level and a category set restriction. For read-access to an item of information, a user must have a clearance level greater than or equal to the classification of the information, and have a category clearance that includes all the access categories specified for the information.

Non-Kernel Security-Related Software (NKSR)—Security-relevant software that is executed in the environment provided by a security kernel rather than as a part of the kernel itself.

Nonrepudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Non-Secret Encryption (CFD)—Synonymous with Public Key Cryptography.

Null—Dummy letter, letter symbol, or code group inserted in an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes.

One-Time Cryptosystem—Cryptosystem employing key used only once.

Open Information System—A communications and information system that is accessed or observed by users outside the system and that provides information by open sources or operational security (OPSEC) indicators. Open information systems use open source information to provide OPSEC indicators that my be observed by adversaries. Open information systems may also be influenced, jammed, interrupted, or exploited by adversaries and adversarial weapons systems. Examples of open information systems are: nonsecured telephone systems, computer systems connected to outside lines, and unsecured radio systems.

Open Security Environment (CFD)—Environment that does not provide sufficient assurance that applications and equipment are protected against the loss of confidentiality, integrity, or availability.

Open Storage—Storage of classified information within an accredited facility, but not in General Services Administration-approved secure containers, while the facility is unoccupied by authorized personnel.

Operational Data Security—Protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, storage, transmission, or output operations.

Operational Key—Key intended for use on-the-air for protection of operational information or for the production or secure electrical transmission of key streams.

Operational Waiver—Authority for continued use of unmodified communications security end items, pending the completion of a mandatory modification.

Operations Security (OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) Identify those actions that can be observed by adversary intelligence systems. (b) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. (c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Optional Modification—National Security Agency-approved modification not required for universal implementation by all holders of a communications security end item. This class of modification requires all of the engineering/doctrinal control of mandatory modification, but is usually not related to security, safety, TEMPEST, or reliability.

Orange Book—The DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).

Organizational Registration Authority (ORA)—Entity within the PKI that authenticates the identity and the organizational affiliation of the users.

Over-The-Air Key Distribution—Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.

Over-The-Air Key Transfer—Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished.

Over-The-Air Rekeying (OTAR)—Changing traffic encryption key or transmission security key in remote crypto-equipment by sending new key directly to the remote crypto-equipment over the communications path it secures.

Overwrite Procedure—Process of writing patterns of data on top of the data stored on a magnetic medium.

Partitioned Security Mode—Information system security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need to know, for all information handled by an information system.

Passphrase—Sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length.

Penetration—1. Unauthorized act of by-passing the security mechanisms of a system. 2. The successful unauthorized access to an AIS or act of by-passing the AIS security controls.

Personal Computer Memory Card International Association (PCMCIA)—The organization of marketing and engineering professionals that defines the architecture of PCMCIA. Also used to refer to the technology.

Periods Processing—Processing of various levels of classified and unclassified information at distinctly different times. **NOTE:** Under periods processing, the AIS (operating in dedicated security mode) is cleared or sanitized (as appropriate) after one processing period before transitioning to the next when there are different users with different authorizations.

Periods Processing—1. Processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next. 2. Processing of various levels of classified and unclassified information at distinctly different times. NOTE**:** Under periods processing, the AIS (operating in dedicated security mode) is purged of all information from one processing period before the next when there are different users with different authorizations.

Permuter—Device used in crypto-equipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits.

Plain Text—Unencrypted information.

Policy Approving Authority (PAA)—First level of the PKI Certification Management Authority that approves the security policy of each PCA.

Policy Creation Authority (PCA)—Second level of the PKI Certification Management Authority that formulates the security policy under which it and its subordinates CAs will issue public keys certificates. Also know as a policy certification authority.

Positive Control Material—Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material, or devices.

Preferred Products List (PPL)—List of commercially produced equipment that meet TEMPEST and other requirements prescribed by National Security Agency. This list is included in the National Security Agency information systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office.

Preproduction Model—Version of Information Systems Security equipment that employs standard parts and is suitable for complete evaluation of form, design, and performance. Pre-production models are often referred to as beta models.

Privacy Protection—Establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records. It also protects both security and confidentiality against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

Private Key—Encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.

Privileged Access—Explicitly authorized access of a specific user, process, or computer to computer resources.

Privileged Data—Data not subject to usual rules because of confidentiality imposed by law, such as chaplain, legal, and medical files.

Privileged Instructions—Set of instructions (e.g., interrupt handling or special computer instructions) to control features (such as storage protection features) that are generally executable only when the computer system is operating in the executive state.

Programmable Read-Only Memory—ROM that can be programmed (written to) once, but not reprogrammed.

Propagation of Risk—Spreading of risk in a network when a system with an accepted level of risk is connected to that network.

Protected Communications—Telecommunications deriving their protection through use of type 2 products or data encryption standard equipment. See Type 2 Product.

Protected Distribution System (PDS)—Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.

Protection Equipment—Type 2 product or data encryption standard equipment that the National Security Agency has endorsed to meet applicable standards for the protection of telecommunications or AISs national security information.

Protection Philosophy—Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

Protection Ring—One of a hierarchy of privileged modes of an information system that gives certain access rights to user programs and processes that are authorized to operate in a given mode.

Protective Packaging—Packaging techniques for communications security material that discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

Protective Technologies—Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

Protocol—Set of rules and formats, semantic and syntactic, permitting information system's to exchange information.

Public Cryptography—Body of cryptographic and related knowledge, study, techniques, and applications that is, or intended to be, in the public domain.

Public Key Certificate—Contains the name of a user, the public key component of the user, and the name of the issuer who vouchers that the public key component is bound to the named user.

Public Key Cryptography (PKC)—Encryption system that uses a linked pair of keys. What one pair of keys encrypts, the other pair decrypts.

Purging—1. Rendering stored information unrecoverable by laboratory attack. 2. The removal of data from an AIS and its storage media in such a way as to provide assurance that the data is unrecoverable by technical means. Purging is the first step in removing classification from media. The other two steps are review of the media, and administrative removal of security classification markings and controls. (See Clearing.)

Quadrant—Short name referring to technology that provides tamper-resistant protection to crypto-equipment.

Radiation—Signals emanating from an equipment that appear as either electromagnetic fields or as spatial longitudinal waves. These include induction field, magnetic field, electric field, and acoustic waves.

Rainbow Series—Set of publications that interpret Orange Book requirements for trusted systems.

Randomizer—Analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator.

RED—Designation applied to information systems, and associated areas, circuits, components, and equipment in which national security information is being processed.

RED/BLACK Concept—Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those which handle non-national security information (BLACK) in the same form.

RED Key—Unencrypted key. See BLACK Key.

RED Line—Any line in which classified or unenciphered signals are carried.

RED Signal—Any electronic emission (e.g., plain text, key, key stream, subkey stream, initial fill, or control signal) that would divulge national security information if recovered.

Rednal—Telecommunications or AIS signal that would divulge classified information if recovered and analyzed. **NOTE:** RED signals may be plain text, key, subkey, initial fill, control, or traffic flow related information.

Reference Monitor—Access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Reference Validation Mechanism—Portion of a trusted computing base whose normal function is to control access between subjects and objects, and whose correct operation is essential to the protection of data in the system.

Release Prefix—Prefix appended to the short title of United States produced keying material to indicate its foreign releasability. "A" designates material that is releasable to specific allied nations and "U.S." designates material intended exclusively for United States use.

Remanence—Residual information that remains on storage media after clearing. See magnetic remanence and clearing.

Remote Rekeying—Procedure by which a distant crypto-equipment is rekeyed electrically. See Automatic Remote Rekeying and Manual Remote Rekeying.

Residue—1. Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place. 2. Data left in storage after automated information processing operations are complete, but before degaussing or overwriting has taken place.

Resource—Any function, device, or data collection that may be allocated to users or programs (i.e., memory, tape drives, disk space, and so forth).

Resource Encapsulation—Method by which the reference monitor mediates accesses to an information system resource. Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.

Risk—Probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis—An analysis of system assets and vulnerabilities to establish an expected loss from test findings and analysis of system documentation (i.e., Trusted Facility Manual , Security Features Users Guide, System Security Architecture, etc.). The purpose of a risk analysis is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

Risk Assessment—Process of analyzing threats to and vulnerabilities of an Information System, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective counter-measures.

Risk Index—Difference between the minimum clearance or authorization of information system users and the maximum sensitivity (e.g., classification and categories) of data processed by the system.

Sample Key—Key intended for off-the-air demonstration use only.

Sanitizing—The removal of information from AIS storage media such that data recovery using known techniques or analysis is prevented. Sanitizing includes the removal of data from the media (purging), verification of the purging action, and removal of all classification labels and markings. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.

Scavenging—Searching through object residue to acquire data.

Scratch Pad Store (SPS)—Temporary key storage in crypto-equipment.

Secret Internet Protocol (IP) Router Network—A High-Speed classified network for DoD that supports GCCS and CIO systems.

Secure Communications—Telecommunications deriving security through use of type 1 products and/or protected distribution systems.

Secure Configuration Management—Procedures appropriate for controlling changes to a system's hardware and software structure to make sure changes will not lead to violations of the system's security policy.

Secure Hash Standard—Specification for a secure hash algorithm that can generate a condensed message representation called a message digest.

Secure Operating System—Resident software controlling hardware and other software functions in an information system to provide a level of protection or security appropriate to the classification, sensitivity, and/or criticality of the data and resources it manages.

Secure State—Condition in which no subject can access any object in an unauthorized manner.

Secure Subsystem—Subsystem containing its own implementation of the reference monitor concept for those resources it controls. Secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects.

Security Architecture—Detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design.

Security CONOPS—A high-level description of how the security of the system operates and a general description of the security characteristics of the system, such as user clearances, data sensitivity, and data flows.

Security Critical Mechanisms—Security mechanisms whose correct operation is necessary to ensure that the security policy is enforced.

Security Domains (Class B3)—Advanced trusted computing base that provides highly effective and mandatory access controls. Significant security and software engineering must be accomplished during the design, implementation, and testing phases to achieve the required level of confidence, or trust. Operational support features extend auditing capabilities as well as other functions needed for a trusted system recovery.

Security Fault Analysis—Assessment, usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.

Security Feature—A hardware, firmware, or software controlled access protection to meet the security requirements of identification; authentication (I&A); mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of automated information system (AIS) security safeguards.

Security Features Users Guide (SFUG)—Guide or manual that explains how the security mechanisms in a specific system work.

Security Kernel—Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Label—Information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security Level—Combination of classification levels and a set of categories, including sensitive unclassified categories, that represents the sensitivity of the information.

Security Measures—The means to protect and defend information and information systems. Security measures include operations security and information assurance.

Security Mode—Mode of operation in which the accredits a computer system to operate. Inherent with each of the security modes are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted in the system. See Mode of Operation.

Security Mode of Operation—Description of the conditions under which an information system operates, based on the sensitivity of information processed and the clearance levels, formal access approvals, and need to know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system-high mode, compartmented/partitioned mode, and multilevel mode.

Security Net Control Station—Management system overseeing and controlling implementation of network security policy.

Security Requirements—Types and levels of protection necessary for equipment, data, information, applications and facilities to meet security policy.

Seed Key—Initial key used to start an updating or key generation process.

Seepage—Accidental flow of data to unauthorized individuals, access to which is presumed to be controlled by computer security safeguards.

Self-Authentication—Implicit authentication, to a predetermined level, of all transmissions on a secure communications system.

Sensitive—Requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity sensitive compartmented information. All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DoD Regulation 5200.1.)

Sensitive Compartmented Information (SCI)—Security classification that includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentation of handling are formally established,

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information are to be protected according to the requirements of the Title 40 U.S.C. 759, *Computer Security Act of 1987*.)

Sensitivity And Criticality Assessment—Study to determine the value of a computer system by taking into account the cost, capability, and jeopardy to mission accomplishment or human life associated with the system.

Short Title—1. Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and control. 2. A short, identifying combination of letters, and/or numbers assigned to a document or device for purposes of brevity and/or security.

Significant Modification—Any modification to the AIS or facility that affects the accredited safeguards or results in changes to the prescribed security requirements.

Simple Security Property—Bell-La Padula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

Single-Level Device—Information system device not trusted to properly maintain and separate data to different security levels.

Sniffer—Software tool that audits and identifies network traffic packets.

Special Mission Modification—Mandatory or optional modification that applies only to a specific mission, purpose, operational, or environmental need.

Split Knowledge—Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams, so that no one individual or team will know the whole data.

Spoofing—Attempt to gain access to a communications and information system by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

Start-Up Key-Encryption-Key (KEK)—Key-encryption-key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.

Structured Protection (Class B2)—Enhanced-level trusted computing base that provides intermediate-level mandatory access control protection features, as well as enhanced DAC features. Sensitivity labels are used to enforce access control decisions and are based on a formally specified security policy model that documents rules for how each subject (users, programs) may access every object (files, records). Operational support features are provided, such as a Trusted Facility Manual, system security officer, and administrator functions, and stringent configuration management practices.

Subject Security Level—Sensitivity labels of the objects to which the subject has both read and write access. Security level of a subject must always be dominated by the clearance level of the user associated with the subject.

Sub-Registration Authority (SRA)—Individual with primary responsibility for managing the distinguished name process.

Superencryption—Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.

Supersession—Scheduled or unscheduled replacement of a COMSEC aid with a different edition.

Superuser—Special user who can perform control of processes, devices, networks, and file systems.

Supervisor State—Synonymous with executive state of an operating system.

Survivability—Capability of a system to accomplish its mission in the face of an unnatural (man-made) hostile, scenario-dependent environment. Survivability may be achieved by avoidance, hardness, proliferation, or reconstitution (or a combination).

Susceptibility—Inability of a system to prevent: (1) An electronic compromise of national security information or, (2) Detrimental effects on its operational integrity.

Suspicious Activity—Suspicious activity includes failed log-ins, changes to privileges, renamed user account or privileges, which may indicate unauthorized access or exceeded authority.

Syllabary—List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. A syllabary may also be a spelling table.

Synchronous Crypto-Operation—Method of on-line crypto-operation in which crypto-equipment and associated terminals have timing systems to keep them in step.

System Administrator (SA)—Individual responsible for the installation and maintenance of an Information System, providing effective information system utilization, adequate security parameters, and sound implementation of established information systems security policy and procedures.

System Development Methodologies—Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

System High—Highest security level supported by an information system.

System High Mode—Information system security mode of operation wherein each user, with direct or indirect access to the Information System, its peripherals, remote terminals, or remote hosts, has all of the following: (a) Valid security clearance for all information within an Information System. (b) Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs). (c) Valid need-to-know for some of the information contained within the information system.

System Integrity—1. Quality of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. 2. The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Low—Lowest security level supported by an Information System.

System Profile—Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an information system.

System Security Authorization Agreement (SSAA)—Applicable set of planning and certification actions, resources, and documentation required to support the certification and accreditation. It guides the implementation of information protection requirements and the resulting certification and accreditation actions.

System Security Engineering—The effort to achieve and maintain optimal security and survivability of a system throughout its life cycle.

System Security Management Plan—Formal document fully describing the responsibilities for security tasks planned to meet system security requirements.

System Security Officer—Synonymous with communications system security officer.

System Security Plan—Formal document fully describing the planned security tasks required to meet system security requirements.

System Security Policy—Set of laws, rules, and practices that regulate how sensitive (SBU and classified) information is managed, protected, and distributed by an AIS. **NOTE:** System security policy interprets regulatory and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks that process SBU or classified information, will have a security policy.

Technical Vulnerability—Hardware, firmware or software flaw that leaves a communications and information system open for potential exploitation. The exploitation can be either from an external or internal source, there by resulting in risk for the owner, user, or manager of the system. Note: The vulnerability must be demonstrable and repeatable, and validated by either the Air Force Information Warfare Center (AFIWC) or a national agency with validation authority.

Telecommunications Security—See Information Systems Security.

Teleprocessing—The combining of telecommunications and computer operations interacting in the automatic processing, reception, and transmission of data and/or information.

TEMPEST—1. Short name referring to investigation, study, and control of compromising emanations from information systems equipment. 2. An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security.

TEMPEST-Certified Equipment—Systems or equipment which were certified within the requirements of the effective edition of NSTISSAM TEMPEST/1-92, Level I, or TEMPEST specifications as determined by the department or agency concerned.

TEMPEST Zone—Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated.

Threat—1. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. 2. Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, or fraud, waste, and abuse to a system.

Threat/Vulnerability Assessment—An observation of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. Managers use the results to develop security requirements and specifications (what do I have versus what do I want).

Ticket-Oriented—Computer protection system in which each subject maintains a list of unforgeable bit patterns called tickets, one for each object that a subject is authorized to access. See List-Oriented.

Top-Level Specification—Nonprocedural description of system behavior at the most abstract level; typically, a functional specification that omits all implementation details.

Traditional Communications Security Program—Program in which the National Security Agency acts as the central procurement agency for the development and, in some cases, the production of information systems security items. This includes the Authorized Vendor Program. Modifications to the Information Systems Security end items used in products developed and/or produced under these programs must be approved by the National Security Agency.

Traffic Encryption Key—Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

Traffic-Flow Security—Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system.

Traffic Padding—Generation of spurious communications or data units to disguise the amount of real data units being sent.

Training Key—Cryptographic key for training.

Transmission Security—Component of communications security resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Transmission Security Key—Key used in the control of TRANSEC processes, such as frequency hopping and spread spectrum.

Trap Door—Hidden software or hardware mechanism used to circumvent security controls. Synonymous with back door.

Trojan Horse—Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.

Trusted Computer System—Information system that employs sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive information.

Trusted Computer System Evaluation Criteria (TCSEC) Nomenclature—System for identifying the type and purpose of certain items of communications security material.

Trusted Computing Base (TCB)—The totality of protection mechanisms within a computer system--including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Distribution—Method for distributing trusted computing base hardware, software, and firmware components that protects the trusted computing base from modification during distribution.

Trusted Facility Management—Administrative procedures, roles, functions, privileges, and data bases used for secure system configuration, administration, and operation.

Trusted Facility Manual—Document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.

Trusted Identification Forwarding—Identification method used in information system networks whereby the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.

Trusted Network—Network that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Path—Mechanism by which a person using a terminal can communicate directly with the trusted computing base (TCB). Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.

Trusted Process—Process that has privileges to circumvent the system security policy and has been tested and verified to operate only as intended.

Trusted Recovery—Ability to ensure recovery without compromise after a system failure.

Trusted Software—Software portion of a trusted computing base.

Two-Person Control—Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

Two-Person Integrity (TPI)—System of storage and handling designed to prohibit individual access to certain communications security keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. See No-Lone Zone.

Type Accreditation—1. Designated approving authority authorization to employ a number of systems in a specified operational environment. To be type accredited, the systems must have similar characteristics, such as same function, physical environment, operating system, security subsystem, and so on. See Accreditation. 2. The official authorization by the accreditor to employ a system in a specified environment. It includes a statement of residual risk, delineates the operating environment, and identifies specific use, operational constraints, and/or procedural work around. It may be performed when multiple platforms will be fielded in similar environments.

Type 1 Encryption Product—Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U.S. Government information, when appropriately keyed. Type I products contain classified National Security Agency algorithms.

Type II Encryption Product—Unclassified cryptographic equipment, assembly, or component, endorsed by the National Security Agency, for use in telecommunications and automated information systems for the protection of national security information. Type II products may not be used for classified information, but contain classified National Security Agency algorithms that distinguish them from products containing the unclassified data encryption standard algorithm.

Type 1 Product—Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified National Security Agency algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

Type 2 Product—Unclassified cryptographic equipment, assembly, or component, endorsed by the National Security Agency , for use in information system for the protection of sensitive unclassified information identified as Warner Amendment (Title 10 U.S.C. Section 2315).

Type 3 Algorithm—Cryptographic algorithm registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) for use in protecting unclassified sensitive information or commercial information.

Type 4 Algorithm—Unclassified cryptographic algorithm that has been registered by the National Institute of Standards and Technology (NIST), but not published as a Federal Information Processing Standard (FIPS).

Unauthorized Disclosure—Exposure of information to individuals not authorized to receive it.

Unclassified—Information that has not been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified.

Untrusted Process—Process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

User Partnership Program—Partnership between the National Security Agency and a U.S. Government agency to facilitate development of secure information systems equipment incorporating National Security Agency-approved cryptography. The result of this program is the authorization of the product or system to safeguard national security information in the user's specific application.

Validation—Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an information system by one or more departments or agencies and their contractors.

Valid Password—Personal password that authenticates the identity of an individual when presented to a password system or an access password that allows the requested access when presented to a password system.

Verification—Process of comparing two levels of an information system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code).

Verified Design—Computer protection class in which formal security verification methods are used to assure that mandatory and discretionary security controls can effectively protect classified and sensitive information stored in, or processed by, the system. Class A1 system is verified design.

Virtual Password—information system password computed from a passphrase meeting the requirements of password storage (e.g., 64 bits).

Vulnerability—1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. Defense weakness to control a threat to the AIS.

Vulnerability Analysis—Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Assessment—Measurement of vulnerability that includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack. **NOTE:** This process may or may not be automated. See Risk Assessment.

Wiretapping—Attaching an unauthorized device, such as a computer terminal, to a communications circuit to gain access to data by generating false messages or control signals, or by altering legitimate users' communications.

Write Down—Ability of a subject to write data to an object that is classified at a lower level than the subject's security level. This is normally not allowed.

Write Up—Ability of a subject to write data to an object that is classified at a higher level than the subject's security level. Permission is provided through the security functions of a system and administered by the system manager.

Zeroize—To remove or eliminate the key from crypto-equipment or fill device.

Zone of Control—Synonymous with Inspectable Space.